ARCADIA UNIVERSITY INTERIM INFORMATION TECHNOLOGY POLICY

INDEX

Policy Title	**Interim[1] Information Technology Policy**
Policy Category	**Information Technology Policies**
Policy Approval Date	**March 29, 2017**
Policies Superseded	**None**
Responsible Office	**Finance**
Related Policies	
Frequency of Review	**3 Years**
Date of Revision	

I. SCOPE

This Interim Information Technology Policy ("Policy") applies to all members of the University Community, as well as, contractors, consultants and all personnel affiliated with third parties using VPN's to access the University network. See Section **IV** for the definitions of all capitalized terms found in this Policy

II. POLICY STATEMENT

This document outlines the University's interim policy regarding Information Technology and articulates the University's vision as it relates to the use of information technology resources, specifies requirements and standards for the consistent use of IT resources throughout the University, and interprets applicable laws and regulations to ensure our use is consistent with legal requirements.

III. POLICY

A. ACCOUNTS MANAGEMENT

Accounts Management applies to the primary credential for authentication to University electronic services and applies only to the uses of the character string as an authentication credential.

The University generates and assigns unique authentication credentials to represent students, faculty, staff, alumni, and other affiliates of the University. The credentials provide electronic access to services, and contain basic identifying information for directory information consistent with federal policy. The credentials position both centrally and locally managed services to authenticate individuals reliably and accurately.

Only one set of credentials is provided to an individual at the time the individual initially assumes or resumes a relationship with the University for which credentials are provided. The credentials remain the property of University and the University reserves the right to change, delete, or add credentials.

[1] This Information Technology Policy is an Interim Policy as defined in the University's Policy for University Policy Development. Interim Policies are policies that may be approved by the President to address matters that require immediate attention or are determined by the President to be in the best interest of the University. Interim policies do not initially utilize the full process for policy development set forth in the Procedures but should undergo full review process within one year of going into effect.

Having a credential is a prerequisite for accessing centrally provided electronic services and is associated with credentials used to authenticate the individual.

Having a credential is not, however, sufficient to authorize individuals to use those services. Each service defines the criteria for service provisioning, and authorizes the Individual according to those criteria.

Having a University credential is a prerequisite to acquiring other central login credentials.

1. Lifecycle

- The credential will be created when an individual initially assumes or resumes a relationship with the University that entitles that person to a credential.
- Because a credential does not require that large numbers of individuals know the credential, the string of characters composing the username will not normally be changed. Requests for changes must be submitted through Human Resources, and will be reviewed by identified University data trustees.
- The credential may be suspended when an individual relinquishes all relationships with the University that could entitle that person to a credential. Human Resources define these relationships. In addition, the University reserves the right to require a renewal process. Renewal criteria may be based upon the elapsed time since a student's last enrollment or a retiree's last employment, the elapsed time since the credential was used for authentication in the Information Technology-provided authentication system and/or additional criteria as determined by the CIO.
- All user accounts that have not been accessed within 180 days will be disabled. All disabled accounts will be deleted after 180 days, if the disabled account is not reactivated. The Office of the Provost will provide a list of adjunct faculty whose accounts should not be deleted. Accounts of individuals on extended leave (more than 180 days) will be disabled. All terminated faculty or staff users accounts will be deleted immediately, unless otherwise instructed by the appropriate vice-president. All accounts of students that are no longer enrolled will be disabled for period of 180 days. If the student does not return to the University within an additional 180 days, the account will be deleted.

2. Character Strings and Namespace

- By using central authentication provided by the University's IT Department, a University electronic service may use the credential and its associated password in a secure and accurate manner. When it is not feasible for a service to use central IT provided authentication, other authentication services should consider using the same character string as the original credential issued by the University.

- If a service requires more than one electronic credential for a given individual, conflict with credentials can be avoided by making a request in electronic form to helpdesk@arcadia.edu, to reserve the character string of the additional electronic IDs in the credential namespace.

3. Passwords

- A minimum credential for logging into electronic services is a password. The CIO establishes the password standards as detailed in the Section M (Password Change) of this Policy.

- Password changes will be accomplished by the user through a process that does not expose the password to being physically read by other individuals, either during the change or after.
- If a password must be administratively reset, then the individual must provide additional information to verify his or her identity. Administrative resetting of passwords will result in a temporary password that must be changed again by the user before it can be used.
- By extension from the Acceptable Use Policy and its associated standard, users must guard their own information associated with password resetting carefully, and not use anyone else's password reset information without permission.
- Passwords for credentials will not be shared with any entity outside the University.
- Additional electronic credentials may be associated with the credential.

B. SERVER PATCH MANAGEMENT

1. Servers. IT is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. IT has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this section will limit the exposure and effect of common malware threats to the systems within this scope.

This section describes IT's requirements for maintaining up-to-date operating system security patches on all Arcadia owned and managed servers. This section applies to servers owned or managed by the University. This includes systems that contain company or customer data owned or managed by IT regardless of location.

Servers owned by the University must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all servers either physical or virtual owned and managed by IT.

Servers must comply with the minimum baseline requirements that have been approved by the CIO. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the <Company Name> asset and the data that resides on the system. Any exception to this section must be documented and forwarded to the CIO for review. See Section 3 below for Exceptions.

2. Monitoring and Reporting. IT is required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk.

3. Exceptions. Exceptions to the patch management require formal documented approval from the CIO. Any servers that do not comply with this section must have an approved exception on file with IT.

C. IT LOANER EQUIPMENT

This section relates to faculty and staff that may need to borrow IT equipment.

The purpose of this section is to clearly outline acceptable uses for loaner equipment, time frames for how long anyone may take out a piece of equipment, and define expectations for handling loaner equipment.

A limited amount of loaner equipment is available from IT. Faculty and staff who wish to take out a loaner must request a loaner through the appropriate request form (see below), or by requesting a piece of equipment at the University Help-desk.

A photo ID must be presented at the time of pickup and return of any loaned equipment.

Generally, technology must be checked out by the User at either the ATS or Helpdesk offices. Delivery is only available for certain items, such as iPad loaners for semester-long courses.

Loaner laptop requests should be made a minimum of two business days in advance. All loaner requests are subject to availability of hardware. Requests should be made as far in advance as possible to guarantee availability.

Available resources include:

- Laptops
- Apple iPads - Two weeks' notice
- Polling Clickers - Same-day checkout available when in stock
- USB Microphones - Same-day checkout available when in stock
- Webcams - Same-day checkout available when in stock
- Swivl - Same-day checkout when available
- Canon HDD Camcorder - Same-day checkout when available

IT staff set maximum loan times for all equipment. This may vary depending on availability and demand of specific hardware. Computers from the Helpdesk@arcadia.edu may be loaned for a maximum of 5 business days. If a laptop or desktop is loaned due to a failure of the user's primary computer, then the loaner may be used until the primary device is returned.

Loaner equipment may not be modified in any way. Any software installs on loaner computers should be completed prior to picking up the device. Loaner hardware should only be used for Arcadia related business and may not be used for recreational or personal use. Software subject to license availability.

All accounts and passwords entered into a loaned device should be removed before return. Users will be expected to come back and remove any accounts or passwords if we are unable to remove them ourselves. The University is not responsible for loss of data or breaches into an account due to not removing an account or purging data from a loaned device prior to return. Users are responsible for backing up their own data. Data stored on any loaner device is not guaranteed to be secure. IT recommends storing data on a University provided network location, external hard drive or online backup service. University is not responsible for damages to person or property caused by a loaned device.

Users are responsible for reporting any equipment theft or damage to the Helpdesk@arcadia.edu or University Public Safety. If hardware is lost or damaged, the faculty or staff department will be required pay the cost of the replacement device or repair.

The University's Acceptable Use Policy must be followed at all times when using any loaner equipment.

****

Faculty/Staff Loaner Equipment Request form

(Will be made into Online form when implemented)

Requestor Name _____

Device Requested _____

Date of Pickup _____

Date of Return _____

Reason _____

_____

Special Instructions _____

I agree to abide by University's the Interim Information Technology Policy and Acceptable Use Policy.

Signature_____

Date: _____

****

D. INFORMATION SECURITY PROGRAM

The University has a highly complex and resource rich information technology environment upon which there is increasing reliance to provide mission critical academic, instructional and administrative functions. Safeguarding the institution's computing assets in the face of growing security threats is a significant challenge requiring a strong, persistent, and coordinated program that leverages widely accepted, effective security practices appropriate for higher education environment. This section states the codes of practice with which the University aligns its information technology security program.

The standards herein establish requirements and general principles for initiating, implementing, maintaining, and improving the University. The program lays out a set of controls that aids in setting objectives on the commonly accepted goals of information security management.

The University considers information to be a strategic asset that is essential to its core mission protecting the information with which it is entrusted. The University also values the privacy of individuals and is dedicated to resources needed to ensure confidentiality, integrity, and availability of its information as well as reduce the risk of exposure that would damage the reputation of the University. The program is designed to support the mission of the University by protecting its resources, reputation, legal position, and ability to conduct its operations. It is intended to help facilitate activities that are important to the University.

The University's information technology security program will be based upon best practices recommended in the "Code of Practice for Information Security Management" published by the International Organization for Standardization and the International Electro technical Commission (ISO/IEC 17799), appropriately tailored to the specific circumstances of the University. The program will also incorporate security requirements of applicable regulations, such as the Family Educational Rights and Privacy Act, the Health Insurance Portability and Accountability Act, and the Gramm–Lech-Bliley Act. Professional organizations, such as the national EDUCAUSE association will serve as resources for additional effective security practices. The program is consistent with and serves to enforce University policies, contracts, agreements, copyrighted files, and other forms of intellectual property; and laws and policies governing student, employee, and other sensitive information, and records retention laws and policies.

The ISO/IEC 17799 Code of Practice and other sources noted above will be used to guide development and ongoing enhancement of additional information technology security policies as needed.

E. NETWORK DEVICE BACKUP

In order to secure critical University data stored on IT network resources, backups must be run on a weekly basis. Critical data must be recoverable in the event of data loss or corruption. Critical data should always be saved to an IT network resource. All backups of critical data must be replicated to an off-site storage location. Network device backups will include only configuration and setup for the device. They will not include firmware or operations system.

The following is a non-exhaustive list of critical devices that must be backed up. Additional devices can be added as necessary:

- Layer 3 switch
- Firewalls
- Access and distribution switch
- Wireless Controllers (access point will not be included)
- Virtual Switching Infrastructure

Devices are to be backed up weekly. Each backup set is retained for a finite amount of time after which it expires and is automatically expunged from all backup systems.

- Weekly Full Backups - will be run every Sunday including all devices. Weekly backups will be retained for one year.
- Monthly Backups, Quarterly Backups, Year End Backups – will be retained according to the Network Data Backup schedule in section F.

F. NETWORK DATA BACKUP

Backups will include only data stored on network resources managed by IT. Data stored on office or personal computers or any other storage location not managed by IT will not be backed up.

In order to secure critical campus data stored on IT network resources, backups must be run on a daily basis. Critical data must be recoverable in the event of data loss or corruption. Critical data should always be saved to an IT network resource. All backups of critical data must be replicated off-site (currently the University colocation data center).

The following is a non-exhaustive list of critical data resources that must be backed up. Additional data sources can be added as necessary:

- Databases and transaction logs
- Lettered drive shares
- User shares
- Application storage
- Virtual Infrastructure
- Websites and related data

Data is backed up on a progressive time scale beginning with daily backups progressing through year-end backups. Each backup set is retained for a finite amount of time after which it expires and is automatically expunged from all backup systems.

- **Incremental Backups** - will be run daily. Daily incremental backups will be retained for two weeks.
- **Weekly Full Backups** - will be run every Friday to include the entire data store. Weekly backups will be retained for two weeks.
- **Monthly Backups** - will be run on a monthly basis at the end of each month. Monthly backups will be retained for one calendar year.
- **Quarterly Backups** - will be run at the completion of every calendar quarter. Quarterly backups will be retained for three years.
- **Year End Backups -** will be run at the end of every calendar year. Year-end backups will be retained for seven years.

G. DESKTOP AND LAPTOP COMPUTER REPLACEMENT AND SUPPORT

1. General

a. The University supports computers used by faculty and staff in computer labs, research labs, the library, and classrooms. All University owned computers contain software licensed by the University. The User Support Team within IT maintains the computers. All problems encountered should be reported to the Helpdesk@arcadia.edu.

b. The University does not support personally owned computers and cannot put University licensed software on personal computers.

c. All computers purchased for a University entity should be requisitioned through IT, regardless of which department is making the purchase. The University works with strict configuration standards to ensure that the device meets the University security and performance requirements, is covered under warranty, and can be supported by University staff. The University also has pre-negotiated pricing on the models most often purchased.

d. IT provides an image of all software on each computer that is covered under an enterprise (University) license on a yearly basis. In some cases, a certain number of computer users are allowed to access software purchased through concurrent licensing. The terms of the license are monitored and enforced by IT. In other cases, software is added to the basic image of a computer to meet a particular academic or administrative need. IT will add this software upon request of the department. IT will always honor the terms of the software license agreement. Questions regarding software should be addressed to the Helpdesk@arcadia.edu.

e. Computer lab computers will generally be replaced every 3 years. Office computers will be replaced every 5 years. Computers that have usable life beyond these dates will be used in department offices for student use, the library, public venues, and other locations.

f. In most cases uses are assigned one computer. When a computer is replaced, the old computer must be returned to IT.

g. Users should not attempt to alter or fix a University owned computer on their own. All support needs should be reported to the helpdesk@arcadia.edu.

h. Users should save all critical work to their network drive share (M:). This ensures that work is copied to the network and will not be lost should the computer drive become damaged or if the computer is stolen or lost.

2. IT Computer Replacement Procedure

a. IT is responsible for the maintenance, replacement and upgrade of the standard-issue computers and computer-related technology equipment used on campus for faculty, staff, and students.

b. In general, equipment that falls under this replacement section includes the one primary computer for full-time faculty and staff as well as general access computers (classroom, public labs, special services, loaners, etc.).

c. When faculty or staff members have multiple computers provided by the University, one computer is designated to be the primary employee computer. This device will be covered under the replacement cycle and its cost assumed by IT if the standardized computer is selected. The primary computer designation will be made by IT in consultation with the faculty member, staff member and either their department chair or supervisor as appropriate. This is the computer that will be tracked for purposes of the replacement cycle. Additional computers may only be replaced using funds from the department for which they were purchased. Computers and devices not designated as the primary device, will not be serviced, or maintained, by IT outside of their manufacture warranty period.

d. Faculty and staff are encouraged to consult with IT regarding both their hardware and software needs. This consultation process should help ensure that all purchases meet faculty and staff needs as well as campus standards.

e. Computer and computer-related technology includes, but is not limited to:

- Desktop computers and workstations in public use labs and classrooms
- Computers used to provide special services
- Loaner equipment
- Computers purchased by IT for use by faculty or staff
- Peripherals required for base-level functionality of these systems (mouse, keyboard, monitor, etc.)

3. Equipment Replacement

a. Faculty and Staff – IT maintains an inventory of all primary computers on campus and the faculty and staff member with whom they are associated. Twice each year (July and December), IT identifies the computers that are due for upgrade based upon the current equipment requirements (age, processor speed, etc.). Those faculty and staff members who have computers that do not meet the current standards will be prioritized according to their computing needs (Software and Hardware limitations, for example). Budget permitting, IT plans to replace computers for faculty and Staff when the computers are 5 years old.

During each replacement cycle (July and December), a standard-issue desktop and laptop configuration for both the Windows and Macintosh platform will be identified by IT. These standard configurations are designed to meet the computing needs for most users. The cost of these standard configurations will be used determine the base value spent on any replacement.

If the standard configuration provided by IT (laptop or desktop) does not meet a user's computing needs, the cost differential between the standard configuration and the user's needed configuration must be assumed by the faculty and staff member's department or other funds available to the faculty/staff

member. If the standard configuration does not meet a user's need, the faculty/staff member must work with IT to develop a configuration that meets their need. This computer should be configured through a vendor approved by IT.

Faculty and staff supervisors must approve the type of computer selected for each user using the Computer Upgrade Supervisor Approval Form (see attached). This form will be distributed to the employee and supervisor when the notice of upgrades is sent.

When any computer is replaced, the computer being replaced must be returned to IT inventory. If a machine returned from a faculty and staff member is capable of fulfilling computing requirements elsewhere within the University this computer may be redistributed to another purpose as needed.

If a faculty or staff member chooses a laptop computer as their primary computer, it will be purchased in lieu of a desktop computer, not in addition to a desktop computer. Since the laptop will be received as a replacement for their existing computer, the existing desktop must be returned to IT inventory for redistribution elsewhere on campus. The laptop may include monitor, keyboard, and mouse, as long as the cost does not exceed the "base value" for the standard upgrades. Otherwise, it is the responsibility of the faculty/staff member or their department to provide the funding for additional peripherals (printers, webcams, speakers, etc.).

Repeat hardware problems or specialized software needs may cause a faculty/staff members primary computer to be upgraded out of cycle at the discretion of IT only if outside of warranty.

Hardware replacements outside of the normal replacement cycle should be requested through the IT Helpdesk by emailing Helpdesk@Arcadia.edu.

b. Staff Only - All Staff must select from the standard Windows Based PC's, unless approved by department head or supervisor.

c. Classrooms and Labs – Budget permitting lectern PCs are replaced on a 3-year cycle. This equipment, in general, is still viable to be redistributed to departments for use in departmental labs, student research, student worker work-stations, or other needed areas.

d. Departmental Labs and Resources – Budget or inventory permitting, IT will make a best effort to provide upgrades to equipment used for departmental labs, faculty research labs, work-study students and other department resources. The equipment used for these upgrades will often be recycled from other areas such as faculty, staff, classroom and/or lab upgrades. These distributions must be requested through the Helpdesk. This service is not guaranteed and performed at the discretion of IT Staff.

This information is provided with the purpose of creating a basic expectation of the lifecycle for computers provided through IT and is not exhaustive in its scope. Any circumstances not covered by this section should be discussed with IT staff.

****

COMPUTER UPGRADE APPROVAL FORM

A signed copy of this form must be completed for all faculty and staff member computer upgrades.

Date: _____

Faculty/Staff Member receiving upgrade: _____

Immediate Supervisor: _____

Computer requested: _____

I approve the above staff member to receive the computer upgrade circled below.

Device Type	Included with Device
Windows 7 Laptop	Dell 5470 Laptop, Docking station, 23” Monitor, mouse and keyboard
Apple Laptop	Apple 13” Macbook Pro with Retina Display 8Gb Ram
Windows 7 Desktop	Dell 3040 Desktop, 23” Monitor, mouse and keyboard
Apple Desktop	Apple Mac Mini, 23” Dell Display, Mouse and keyboard
Other	

If other is selected, the computer must be approved by IT and purchased using a University-approved vendor. Work with Help-desk staff to configure and order this device. Additional charges to your department may be required.

Supervisor's Signature:

By: _____

Date:_____

****

PC Image Preload Directory

Software

- Office 2016
  - Word
  - Excel
  - Powerpoint
- Adobe Reader
- Chrome
- Firefox
- Symantec Endpoint
- Inventory Agent (Kace)

Codecs/Runtimes

- Silverlight
- Air
- Java
- Flash
- Quicktime
- VLC
- Microsoft .Net 4.5.2

Drivers

- None

H. DATA CLASSIFICATION

This Data Classification section covers all data produced, collected or used by the University, its employees, student workers, consultants or agents during the course of University business. The purpose of this section is to identify the different types of data, to provide guidelines and examples for each type of data, and to establish the default classification for data. It is the decision of the University to classify all data covered by this section as Institutional Data, Sensitive Data, or Public Information (defined below).

1. Data Classification Types

All data covered by the scope of this section will be classified as Institutional Data, Sensitive Data, or Public Information.

- Institutional Data: Institutional Data is any information, including Directory Information, PII, and Student and Employee Financial Information, and Public Information that can be linked to any individual, including but not limited to, students, faculty, staff, patients, or contractors. Institutional data and all applications storing and transmitting such data, regardless of the media on which they reside, are valuable assets, which the University has an obligation to manage, secure, and protect.
- Sensitive Data: Sensitive Data is any data that is not classified as Institutional Data, but which is information that the University would not distribute to the general public. Examples of the types of data included are: budgets, salary information, physical resource data, financial data, University contracts; research data, etc.

- Public Information: Public Information is information, including directory information (unless a student has expressly requested non-disclosure pursuant to the University FERPA Policy) that is available to the general public. Examples of the types of data included are: department faculty lists, department addresses, press releases, and the University website. Any data that does not contain PII concerning any individual, and that is not Institutional Data or Sensitive Data, must be classified as Public Information.

2. Default Classification of Data

Any data that contains PII concerning any individual or that is covered by local, state, or Federal regulations, or by any voluntary industry standards concerning protection of personally identifiable information that the University chooses to follow, is automatically classified as Institutional Data. All other data is classified as Sensitive Data by default.

I. ELECTRONIC MAIL

A. General

This Electronic Mail section applies to all Authorized Users who are issued a formal University email account. The purpose of this section is to establish the University's policy and procedures regarding the use of University email facilities. Authorized users of University email facilities are responsible for using and maintaining their email account in accordance with the procedures and guidelines set forth in this section.

Electronic mail, like postal mail, is an official means for communicating University business. All students, faculty and staff are expected to read, and shall be presumed to have received and read, all email messages sent to their official University email account.

Policies and regulations that apply to other forms of communications and the use of Technology Resources also apply to email facilities. In addition, the following specific actions and uses of University email facilities are improper:

- Any use of email that interferes with University activities and functions or does not respect the image and reputation of the University.
- Concealment or misrepresentation of names or affiliations in email messages.
- Alteration of source or destination address of email.
- Use of email for commercial or private business purposes that have not been approved by the administration.
- Use of email to send mass or chain messages in violation of Section IB (Mass Email) below.
- Use of email for organized political activity or political solicitation.
- Use of email in violation of the University Acceptable Use Policy.
- Use of email to harass or threaten other individuals in violation of the University Non-Discrimination and Non-Harassment Policy or Policy Prohibiting Sexual Misconduct, Relationship Violence, and Stalking.

Authorized Users of the University's email facilities whose actions violate this section or any other University policy or regulation may be subject to revocation or limitation of email privileges as well as other disciplinary actions or may be referred to appropriate external authorities.

The University respects the privacy of its email users. It does not routinely inspect, monitor, or disclose email. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this section, the University may deny access to its email services and may inspect, monitor, or disclose email in accordance with the University Acceptable Use Policy.

Email, whether or not created or stored on University Technology Resources, may constitute a University record subject to disclosure or other laws, or as a result of litigation. However, the University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of laws concerning disclosure and privacy, or other applicable law. Destruction of such records shall be governed by Section EE (Records Retention) of this Policy.

B. Mass Email

1. General.

This section provides guidelines for the distribution of e-mail to University domestic faculty, domestic staff, international faculty and staff, alumni, graduate and undergraduate students, and the four current classes of undergraduate students. IT creates and maintains the following campus e-mail lists: domestic faculty, domestic staff, graduate students, and undergraduate students.

All e-mails targeted to one or all of the groups noted above must be sent from an IT-created and approved e-mail account. E-mail should not be sent to the main distribution lists from any other e-mail account.

In order to maintain the utility of the University's mass e-mail system and to reinforce network security best practices, the following criteria have been established for mass e-mail distribution:

- Messages must directly relate to carrying out the business of the University, or
- Messages must share information related to time sensitive issues that affect a significant number of campus community members, or
- Messages must inform a pre-defined target group of an announcement or event related to their specific role within the University, or
- Messages must relate to significant campus disruptions or occurrences.

Announcements that do not meet the above criteria of urgency and/or deliver critical University information will not be distributed via mass e-mail. Additionally, inappropriate uses of mass e-mail include:

- Messages that are not aligned with the mission of the University,
- Messages that are personal in nature,

- Messages that are commercial in nature, with the exception of those messages that are in support of University business, and
- Messages that solicit participation in, support of, or advocacy for events, activities, or campaigns that are not aligned with and/or sanctioned by University.

Departments or campus groups may create smaller group e-mail lists for their business purposes. Only personnel authorized by the vice president to whom they report and only for appropriate group business should use these group e-mail lists.

2. Procedure

a. The initial request for approval must identify the pre-defined target audience.

b. Brevity is encouraged in composition of mass e-mails.

c. Sending multiple mass e-mails about the same subject on different occasions is strongly discouraged, in most instances, and should only be approved under special circumstances.

d. The request will be reviewed by the Office of University Relations and sent for approval, if it meets the criteria above, to the appropriate vice president.

e. Once a proposed mass e-mail receives vice presidential approval, it will be processed and distributed by the Office of University Relations.

f. Under emergency circumstances, designated representatives of University Public Safety, Information Technology, and Facilities may bypass these procedures in order to deliver necessary information as rapidly as possible.

C. Email Retention

This section applies to all University email accounts provided through the University's email server. The purpose of this section is to establish the University's procedures regarding the retention of the University emails on the Microsoft Exchange server. Authorized Users of the University's email service are responsible for maintaining their email accounts in accordance with this Policy. IT will implement automated data purge mechanisms in the University's email service.

1. Individual users (senders, recipients) are responsible for identifying and archiving information in their University email subject to the University Record Retention Schedule set forth in section EE below, or in order to maintain compliance with applicable Federal or state laws or University policies.

2. Retained Records email messages shall be retained according to the University's Records Retention Schedule.

3. Lasting Value email messages are messages that have been under retention schedule requirements, and the active retention period for a particular record in email format has expired. Lasting Value email messages may be retained when useful to the user, but should be removed when the message becomes designated as Transitory.

4. Transitory messages shall be removed promptly from the University's email infrastructure by moving the message into either Trash or Spam folders. The University automatically and permanently deletes messages placed into the Trash or Spam folders after 30 days.

5. A litigation hold directive overrides this section until the hold has been cleared.

6. Emails containing PII shall not be stored, transmitted, or processed using email infrastructure unless appropriate information security mechanisms (e.g. message encryption) are employed.

7. For an employee who is terminated, the employee's supervisor is responsible for evaluating the employee's email records for required retention, in the course of the termination process, and taking appropriate action to retain email as required. After 30 days post termination, the terminated employee's account will be permanently deleted.

8. Users are permitted to forward email to a non-University email service. All official email correspondence, however, is to be performed from a University email account.

J. REMOTE ACCESS (VPN)

This Remote Access (VPN) section applies to all University employees, students, contractors, consultants, and all personnel affiliated with third parties using VPNs to access the University network. The purpose of this section is to state the requirements for remote access to computing resources hosted at University using remote access technologies. These requirements are designed to minimize the possibility of information disclosure to unauthorized parties, while still providing necessary informational resources to the University community. Authorized Users may use the benefits of the University's provided VPN technology. The VPN connection requires appropriate University login credentials as defined in section III A (Accounts Management).

1. Requirements

- Authorized Users must use University provided VPN technology as outlined in the VPN Standards (see 2 below).
- Secure Remote Access is enforced via the University's VPN gateway.
- Authorized Users may not provide their Log-in Credentials to another person.
- People and entities with Remote Access privileges must ensure their University-owned/leased or personal computer or Mobile Device is not connected to another network while it is connected to the University's private network.
- All systems connected to the University's non-public networks via Remote Access must meet security standards established by IT.
- Departments or individuals who wish to implement non-standard Remote Access solutions to the University's network must obtain prior approval from the CIO.
- Current University Employees, excluding student workers, have permission to access the VPN, solely for the purpose of conduct University business. Access by student contractors, and consultants is permitted on a case by case basis as assessed by IT.
- All computers and Mobile Devices connecting to the University's VPN must have active, up-to-date antivirus software and operating system patches.

2. VPN Standards

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to the University's network and to otherwise exercise

caution. Care is required not to expose confidential University information or student or employee information that is protected by privacy laws or policies.

- When actively connected to the University network, the VPN will force all traffic to and from the host over the VPN tunnel: all other traffic will be dropped.
- Dual (split) tunneling is not permitted; only one network connection is allowed.VPN gateways will be set up and managed by IT.
- All hosts that are connected to the University's network via remote access must meet the configuration requirements established by IT.
- VPN users will be automatically disconnected from University's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- Only IT approved VPN clients may be used.
- By using VPN technology with personal equipment, Authorized Users must understand that their machines are a de facto extension of the University's network, and as such are subject to the same rules and regulations that apply to University-owned/leased equipment, i.e., their machines must be configured to comply with University policies.

K. ENCRYPTION

This section applies to all employees, faculty and staff, student workers including interns whose job function falls within scope of this section by virtue of the types of data access, which they are granted, either explicitly or implicitly; and, all contractors, vendors and any other third parties entrusted with Institutional Data. The purpose of this section is to establish the types of devices and media that need to be encrypted, when encryption must be used, and the minimum standards of the software used for encryption. It is the decision of the University to employ encryption to mitigate the risk of disclosure or alteration of Institutional Data within the University's Technology Resources infrastructure or through outsource services. Moreover, it is a violation of this section for anyone to attempt to disable, remove, or otherwise tamper with University installed encryption software.

1. Devices and Media Requiring Encryption

Encryption is required for all laptops, workstations, Mobile Devices, and portable drives that may be used to store or access Institutional Data. Encryption is recommended for all laptops, workstations, and portable drives that may be used to store or access Sensitive Data.

IT will provide, install, configure, and support encryption where it is needed. Departments who have a laptop, workstation, Mobile Device, or portable drive that needs to be encrypted should contact IT. Authorized Users are also responsible for reporting any known, unencrypted Institutional Data on such devices to IT and request assistance in removing the data or acquiring encryption software.

2. Electronic Data Transfers

Any transfer of unencrypted Institutional Data or Sensitive Data must take place via an encrypted channel. Encrypted Institutional Data or Sensitive Data may be transmitted via encrypted or unencrypted channels. All email communications that involve email addresses outside of University use an unencrypted channel, and therefore require that messages containing Institutional Data or Sensitive Data be encrypted. Approved methods of encrypting electronic data transfers include:

- Transport Layer Security (TLS1.1 TLS1.2);
- SSH File Transport Protocol (SFTP); and
- Connecting via an ITS-approved Virtual Private Network (VPN).

If the encryption method includes a password, that password must be transferred through an alternative method, such as speaking with the intended recipient (but not leaving the password on voice mail. Email messages containing encrypted data may never include the password in the same message as the encrypted data. Individuals who are unsure if they are correctly encrypting electronic data transfers should contact IT.

3. Physical Transfer of Electronic Data

Any time Institutional Data or Sensitive Data is placed on a medium such as a CD, DVD, or portable drive to facilitate a physical transfer, either entirely within the University or between the University and a third party, that data must be encrypted. Archiving Institutional Data or Sensitive Data to a physical medium is not recommended, but is permitted if the data is encrypted. All archiving should be done electronically, so that it is stored in a controlled data center and backed up by IT.

4. Software

IT will install software that is capable of encrypting the entire hard drive on all University-owned or leased computers and Mobile Devices identified by the University's CIO as containing Institutional Data. Users who require encryption software should contact IT to arrange installation of encryption software.

5. Institutional Data

Institutional Data is any information, including Directory Information, PII, and Student and Employee Financial Information, and Public Information that can be linked to any individual, including but not limited to, students, faculty, staff, patients, or contractors. Institutional data and all applications storing and transmitting such data, regardless of the media on which they reside, are valuable assets, which the University has an obligation to manage, secure, and protect.

6. Sensitive Data

Sensitive Data is any data that is not classified as Institutional Data, but which is information that the University would not distribute to the general public. Examples of the types of data included are: budgets, salary information, physical resource data, financial data, University contracts; research data, etc.

7. Public Information

Public Information is information, including directory information (unless a student has expressly requested non-disclosure pursuant to the University FERPA Policy that is available to the general public. Examples of the types of data included are: department faculty lists, department addresses, press releases, and the University website. Any data that does not contain PII concerning any individual, and that is not Institutional Data or Sensitive Data, must be classified as Public Information.

L. DIGITAL MILLENNIUM COPYRIGHT ACT

1. General

The purpose of this section is to address the University's compliance with the Digital Millennium Copyright Act (DMCA) and specifically 17 U.S.C. Section 512(c), as amended. The University respects the rights of copyright holders, their agents and representatives, and implements appropriate policies and procedures to support these rights without infringing upon the legal use, by individuals, of those materials. All individuals who use University Technology Resources are responsible for their compliance with applicable copyright laws, University policies, and other applicable provisions. Under appropriate circumstances, the University may terminate authorization of users of its system or network who are found to intentionally or repeatedly violate the copyright rights of others.

The University's designated, registered DMCA Agent (defined below) shall receive all claims of

infringement under the DMCA. Claims may come from inside or outside the University. The DMCA Agent shall promptly acknowledge receipt of each infringement claim, process, investigate, and take appropriate actions under the DMCA.

The DMCA Agent shall coordinate activities, keep required records, and assure proper adjudication of incidents in conformity with University policies and procedures and applicable legal provisions.

The University will use a three-pronged approach to address DMCA related activities. The University will: 1) provide annual disclosures to students about copyright law, policies, and penalties, as well as education on DMCA issues; 2) use reasonable measures to prevent inappropriate use of peer-to-peer (P2P) programs and software, including technology methods; and 3) annually suggest lawful alternatives for obtaining electronic copyrighted materials.

The DMCA provides an opportunity for college and universities to shield themselves from liability for the actions of users that infringe on the copyrights of others. Any use of the Technology Resources to illegally transfer copyrighted material including, but not limited to, software, text, images, audio and video is strictly prohibited.

Under the DMCA, the University will not be liable to the individual using electronic information for any harm they might suffer because of its actions in disabling access so long as it:

- Takes reasonable steps to notify the individual about the allegations in a conforming notice that was received;
- Promptly sends a copy of any substantially conforming counter-notice to the complainant indicating that it will restore access in 10 business days; and
- Restores access to the allegedly infringing work within 10 to 14 business days after the day it receives the counter-notice, unless it first receives a notice from the complainant that they have filed an action seeking a court order to restrain the page owner.

2. Notices and Takedown Requests

In accordance with the DMCA, University has designated the CIO as the DMCA Agent to receive and respond to reports of alleged copyright infringement. This designation is listed on the University's public facing website. DMCA notices and takedown requests must be routed to the University's DMCA Agent.

The DMCA specifies that any DMCA notice or takedown requests must be in writing (either on paper or electronic mail) and must include the following elements: a physical or electronic signature; description of the work claimed to be infringed; description of the allegedly infringing work and the location on the University's public facing website; contact information for the complaining party; a statement that the complaining party has a good faith belief that the use of the material in the manner complained of is not authorized by the copyright owner or law; a statement that the information contained in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the copyright owner. Failure to include information required by the DMCA in the notice of alleged infringement may result in a delay of the processing of the DMCA notification. The University reveals names of alleged offenders only when provided a valid subpoena.

Upon receipt of a DMCA notice or takedown request, the University's DMCA Agent or designee will follow the takedown procedure outlined in the Digital Millennium Copyright Act – US Copyright Law, Chapter 5, section 512(c)(3). In addition, the DMCA Agent or designee will notify the individual responsible for the content that the takedown has taken place, and inform them of their rights regarding counter-notice and put back procedures, which are outlined in the Digital Millennium Copyright Act – US Copyright Law, Chapter 5, section 512(g).

3. Enforcement

Any use of Technology Resources to illegally transfer copyrighted material including, but not limited to, software, text, images, audio and video may lead to serious consequences, including disciplinary action, suspension, and possible lawsuits resulting in substantial financial penalties.

Upon identification of reasonable facts to pursue discipline, the DMCA Agent, or designee, will process the information through the applicable disciplinary process for determination of responsibility. The individual's supervisor or [student life official] as applicable will be notified of the alleged copyright violation notice.

M. PASSWORDS

1. General. This section applies to all Authorized Users accessing the University's Technology Resources regardless of their capacity, role or function including, but not limited to, students, faculty, staff, third party contractors, visitors (guests), consultants, and employees fulfilling temporary or part-time roles. The purpose of this section is to establish a standard for creation of strong passwords, the protection of those passwords, and the procedures and guidelines for resetting passwords. It is the policy of University that anyone who has been issued authentication credentials for an account on any Technology Resource system, has access to the University network, or stores any non-public Institutional Data adhere to the password policy guidelines set forth in this Policy. At no time should an Authorized User grant access to the user's account by providing someone else the password.

Passwords are an important aspect of computer security. A poorly chosen password may result in the compromise of the University's entire network. The purpose of having a password policy is to ensure a more consistent measure of security for the University's network and the information it contains. The implementation of this Policy will better safeguard Institutional Data. Additionally, this section establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of passwords. Accordingly, the University has established the following policy guidelines regarding the use of passwords:

2. Generating Passwords

All passwords must have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z);
- Have digits and punctuation characters as well as letters (e.g., @$&"(), <>`;=#; dash, underscore, pound, etc.);
- Are at least eight characters in length;
- Are not a word in any language, slang, dialect, jargon, etc.;

- Cannot contain user's name (last or first) and must not be based on personal information, names of family, etc.;
- Passwords must never be stored on-line. When writing passwords down, keep them in a secure place that is not easily accessible to others.

3. Protecting Passwords

All passwords are to be treated as sensitive, confidential University information. Do not:

- Use the same password for University accounts as for other non-University accounts (e.g., personal ISP account, option trading, benefits, etc.),
- Share University passwords with anyone, including administrative assistants or secretaries,
- Reveal a password in an email message,
- Talk about a password in front of others,
- Hint at the format of a password (e.g., "my family name"),
- Reveal a password on questionnaires or security forms,
- Share a password with family members,
- Use the "Remember Password" feature of applications (e.g., Firefox, Thunderbird.),
- Store passwords in a file on any computer system without encryption.

If an account or password is suspected to have been compromised, report the incident to IT and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the Authorized User will be notified and required to change it.

4. Password Expiration

All passwords will be scheduled to expire 180 days from the date they were last set.

Advance warnings of upcoming password expiration will be sent to the account holder via campus email beginning 30 days prior to expiration, with repeated reminders thereafter until the expiration date or until your password is changed. An account holder may change a password at any time -- it is not necessary to wait for expiration.

Please note that no data will be lost between the time a password expires and the time it is reset. Email accounts will continue to receive messages during this period but existing mail will not be accessible and new mail will not be able to be sent out.

5. Enforcement. Individuals violating this section may have their account either suspended or terminated given the severity of the offense. Refer to the enforcement section of the University's Acceptable Use Policy for additional information.

N. SECURITY RESPONSE PLAN.

The University's Information Technology Security Incident Response Plan (Plan) applies to University departmental information security contacts and systems administrators with direct involvement in the identification and resolution of security incidents on the Technology Resources, which they manage.

The Plan defines standard methods for identifying, documenting and responding to data security incidents. The University's Plan identifies and describes the roles and responsibilities of the University's Incident Response Team, which is responsible for activating the Incident Response Plan.

1. Identification of Incident

Any user or individual or organization not affiliated with University may refer a data security incident to the University's CIO. The CIO and designated personnel can identify a data security incident through proactive monitoring of University's network and information system activities.

2. Establishment of Incident Response Team

The CIO shall assemble, manage, maintain, train, and lead the incident response team. Refer to the definitions section for a listing of members of the response team.

3. Containing Damage and Preserving Evidence

Following a data security breach the Incident Response Team will:

- Review the circumstances and the actions taken,
- Assign roles,
- Create a plan of action to contain damage and gather evidence;, and
- Ensure that wherever possible, a forensic copy of the affected computer hard drive or server database is created.

The incident response team will work with the appropriate staff and IT to take whatever actions are necessary to ensure that no additional institutional data is lost or taken and/or that no additional information technology is exploited.

4. Incident Response Report

The incident response team will ensure that data security incidents are appropriately logged and archived. To that end, following any data security incident, the incident response team must produce an incident response report as outlined herein. Any data security incidents involving Electronic Protected Health Information (ePHI) pursuant to the Health Insurance Portability and Accountability Act (HIPAA) will be so identified in the report. The incident response team will be responsible for communicating the incident to appropriate University personnel and maintaining contact, for the purpose of update and instruction, for the duration of the incident.

Each report should include at a minimum the following:

- A description of the data security incident,
- Type of institutional data or other information exposed and/or potentially at risk of exposure from the data security incident,

- Type of University information technology damaged or potentially at risk of damage or loss due to the data security incident,
- Steps taken for containment of the data security incident,
- Steps taken for remediation of the data security incident,
- Logging of all internal and external communications issued, including all emails and phone calls regarding the data security incident,
- Interactions with law enforcement and disciplinary University authorities regarding the data security incident, and
- Legal obligations and actions taken to satisfy those legal obligations regarding the data security incident.

5. Additional Obligations of Incident Response Team

Simultaneous with the creation of the report and containment of the data security incident, the incident response team must:

- Determine how the data security incident occurred and take immediate remedial action to prevent it from occurring again,
- Collaborate with University's outside counsel to determine and then perform University's obligations to affected persons and parties,
- Collaborate with the president and office of University communications to manage public relations communications effectively regarding the data security incident;, and
- Rebuild all comprised University Information Technology and closely monitor the rebuilt systems.

6. Incident Prevention

Wherever possible and in conjunction with the application of other University policies relating to information security, University will undertake to prevent data security incidents by monitoring and scanning its own network for anomalies, and developing clear protection procedures for the configuration of its information technology and other related resources.

7. Modifications and Adjustments

This Plan and its procedures will be reviewed periodically to adjust processes, identify new risks and remediation.

8. Special Situations/Exceptions

Any personally-owned devices, such as Smartphones, tablets, wireless devices or other electronic transmitters which have been used to store institutional data and are determined to have contributed to a data security incident, may be subject to seizure and retention by University authorities until the data security incident has been remediated, unless the custody of these devices is required as evidence for a court case. By using these devices within the University network for business purposes, individuals are subject to University policies restricting their use such as the University Acceptable Use Policy.

O. ANTI-VIRUS GUIDELINES

1. Recommended processes to prevent virus problems:

- University licenses anti-virus software for all University owned and student computers. Faculty and staff have the software pre-loaded when they receive their computers. Students may download the software from the MyArcadia portal.
- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then be sure to empty your recycle bin or trash.
- Delete spam, chain, and other junk email without forwarding, in keeping with AU's Acceptable Use Policy.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a requirement to do so.
- Always scan external drives such as usb hard drives or flash media from an unknown source for viruses before use.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place. The University provides a network drive (M:) for this purpose.
- If lab-testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the antivirus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. New definitions will be downloaded to your computer as they are released by enterprise anti-virus provider generally daily.
- Users of University hardware are not permitted to remove or uninstall the Antivirus software themselves. If you experience issues with this software, contact the Help Desk.

P. COPYRIGHT AND INTELLECTUAL PROPERTY

The University respects original authorship of all professional works including the written word, audio, and video. The University prohibits the use of its computer resources to conduct any illegal activity. The University reserves the right to block access to the University network systems for any member of the University community who participates in behavior that is prohibited by the University's policies or federal, state or local laws.

1. Copyright Law

The University affirms its commitment to comply with United States law relating to copyright; to respect the property rights of authors and their assignees; to educate members of the campus community about copyright law; and to exercise vigorously the rights and responsibilities granted under this law.

This section adheres to the long-standing academic tradition that creators of works own the copyright in works resulting from their scholarly, pedagogical, and creative activities. This principle is the foundation of this policy on copyright. This principle also underlies the commitment of University to fostering an environment of respect for and responsible use of the intellectual property of others. University is committed to helping members of the community comply with copyright laws by providing

resources to help individuals make informed, careful, and situation-sensitive decisions about the lawful and fair use of work created by others.

2. Application

This section applies to all members of the University community (faculty, students and staff) who use computing resources, information technologies, networks, voice messaging equipment, computer software, data networking equipment, including remote and wireless and electronically stored Institutional Data (defined in K above) and messages owned or managed by University or third parties contracting with University for the provision of hosting, network or other technology services (hereafter "users"). Any person who has agreed to the University Acceptable Use Policy has, in effect, agreed to this copyright section.

It is the policy of University that all users must comply with U.S. Copyright Law. The owner of the copyright on the materials may copy copyrighted materials freely. In addition, copyright holders such as scholarly publishers, may explicitly release their published materials from strict observance of copyright laws for stated classroom or research purposes.

3. Compliance with Copyright Laws

Using a computer to copy, or store any copyrighted material (text, images, music, movies, etc.) without authorization is a violation of the law, and leaves you liable, for conviction to imprisonment, heavy fines, and or damages. Owners of copyrighted materials have become much more assertive of their rights recently, and are taking legal action against those whom they believe are violating their copyrighted property. For more information about copyright law see www.copyright.gov.

Before relying on fair use exceptions to the Copyright Act, users should educate themselves regarding the limits of fair use and should, in each instance, perform a careful, good faith fair use analysis based on the factors identified in Section 107 of the federal Copyright Act.

Faculty and staff are permitted to use and duplicate copyright materials of other parties for educational and classroom uses, provided such activities are within the fair use standard. The fair use standard requires consideration and balancing by users of the following factors to determine if duplication or use by a third party constitutes fair use.

4. The Fair Use Factors

a. *The Purpose and Character of the Use, Including whether the Use is of a Commercial Nature or is For Non-Profit Educational Purposes*: A non-profit use weighs in favor of fair use. Non-profit educational purposes, such as duplication for classroom purposes rather than commercial purposes, generally tend to support a finding of fair use.

b. *Nature of the Copyrighted Work*: Works fall into categories such as published or unpublished, fact or fiction. Published factual works, such as form books, dictionaries or other factual works, by their nature more readily support a finding of fair use than do unpublished works or non-factual, fictional, creative works.

c. *Amount and Substantiality of the Portion Used in Relation to the Copyrighted work as a Whole*: If the portion of the work copied or used in relation to the entire work is quantitatively and qualitatively insignificant that supports the finding of fair use. No specific number of words or percentage copied of the work is set as being permissible. However, see the "safe harbor" guideline discussed. Copying of a minor part of a work may be found to be other than fair use if the portion constitutes the essence or critical part of the copied or used work. Users should post links to articles and materials whenever possible rather than duplicating complete works.

d. *The effect of the Use upon the Potential Market for or Value of the Copyrighted Work:* This factor is considered the most important element to be considered under the fair use analysis. Duplication or use of copyrighted work that is not detrimental to and does not diminish the potential market for the work will support findings of fair use.

Examples of Acts that do Not Constitute Fair Use:

- Duplication of materials for profit
- Duplication of material from published textbooks
- Duplication of unpublished materials
- Duplication of computer software for multiple use
- Duplication of the same materials for classroom use term after term

5. File Sharing and Peer to Peer Software Programs

Current technology easily allows personal computers to duplicate and distribute copyrighted video images, audio recordings and other digital material. Unfortunately this makes it easy violate the University policy and US Copyright Law. For this reason the use of popular and freely distributed file sharing programs creates a violation of University policy and US law.

Most file sharing programs by default allow Internet users to copy files from a computer. Most programs do not provide alerts in advance or even ask the users permission before turning a computer into an Internet file server. Some of these programs install hidden components that allow file sharing to run in the background on a computer. As a result, whenever a computer is turned on, the file sharing application is also enabled, even if the application is not opened or actively used. Such an application places a user at a high risk of violating the University policy and copyright law by becoming an unlawful distributor of copyrighted material. Because University has a reliable and large capacity connection to the Internet and because these file sharing programs favor computers connected to fast reliable networks, thousands of other Internet users flock to your computer to download your file.

University does not monitor computer use on the University network to look for copyright violations; however, in the process of investigating network congestion or troubleshooting technical problems, University may become aware of policy violations. In such cases immediate action will be taken but University, including disconnection of network access.

Law enforcement agencies, the Recording Industry Association of America and other copyright holders of digital media are actively monitoring the Internet for users who are distributing copyrighted materials. The recording, film and software industries have become very aggressive in their pursuit of copyright infringement.

6. Software Generally Protected by Copyright Law

Copyright law protects the vast majority of all computer software. The few exceptions to this rule are so few that users should assume that all software is protected, unless there is a clear indication to the contrary.

Simply stated, possessing software for which an individual does not own a license is a violation of the Copyright Act, and may subject both the University and the individual user to sanctions set forth in the Copyright Act. For all practical purposes, the fair use exception does not apply to operating system and application software.

In addition to application software and operating systems, federal copyright protection also extends to the data files (content) created for use with or by the applications and operating systems. Unauthorized creation, copying, and distribution of these materials are violations of the federal copyright statute, unless they can be construed as fair use.

7. Violation of Copyright Laws

Upon obtaining knowledge that material residing on its systems or networks is infringing or that its systems or networks are being used for infringing activities, University will act quickly to remove or disable access to the infringing materials and may deny the users responsible further access to its systems or networks. In addition, users who willfully disregard or violate copyright law may be subject to disciplinary action in accordance with applicable disciplinary policies and procedures.

The University Acceptable Use Policy and the University copyright policy state the receipt of, possession of, or distribution of copyrighted materials without the permission of the copyright holder is prohibited. Such acts are in violation of the laws of the United States (Title 17, US Code). Violators of copyright law could be subject to felony charges in state and federal court, and may also be sued by the copyright holder in civil court. Such civil suits could subject the violator to liability for infringement with damages up to $100,000 per work.

8. Digital Millennium Copyright Act

President Clinton signed the Digital Millennium Copyright Act (DMCA) into law in October 1998. One of the provisions of the legislation provides an opportunity for universities such as University to shield themselves from liability for the actions of users that infringe on the copyrights of others. Any use of the University network, email system, or web sites to transfer copyrighted material including, but not limited to, software, text, images, audio and video is strictly prohibited. As indicated above, acts of piracy are violations of state and federal laws and as such may result in criminal changes.

9. TEACH Act

The Technology, Education and Copyright Harmonization Act (TEACH Act) (section 110(2) of the US Copyright Law) is a copyright exemption that addresses teaching conducted through digital transmission.

Under the TEACH Act, instructors may use the following copyrighted materials when teaching a class through digital transmission:

- Performance of non-dramatic literary works,
- Performance of non-dramatic musical works,
- Performance of any other work, including dramatic works and audiovisual works, but only in "reasonable" and "limited portions", and
- Displays of any work "in an amount comparable to that which is typically displayed in the course of a live classroom session".

When using the copyrighted materials above in a digital transmission, the instructor has the following obligations under the TEACH Act:

- The performance is made by or under the supervision of an instructor,
- The use is limited to performances and displays. The TEACH Act does not apply to material that are for student independent use and retention, such as textbooks or other readings,
- The work is a part of systematic mediated instructional activities;
- The transmission must be made solely for and limited to students officially enrolled in the course,
- Only lawfully acquired materials may be used,
- The instructor should use reasonable efforts to prevent copying and retention of the work (e.g., streaming for video, thumbnails, watermarks and disabling right click copy function for images),
- The materials used should not include those primarily marketed for the purposes of distance education (e.g., and electronic textbook or multimedia tutorial,
- A digital copy may be made from analog copy when no digital version is available or when or when the digital version is electronically protected, and
- The work must carry a notice to students that the works are copyrighted.

Instructors should also be mindful that they might also consider fair use when using copyrighted works in distance education settings. See Compliance with Copyright Law above for additional information.

10. Use of copyrighted video

University students, faculty, and staff should be aware that it is a violation of federal law and to improperly present video materials. Those who show videos for entertainment purposes without permission from the licensee in a public area are in violation of the copyright law and University copyright policy. This restriction applies even if there is no admission charge for the performance. Using copyrighted material in a private or classroom showing for educational purposes is not in violation of the law.

Q. IDENTITY THEFT PREVENTION (RED FLAG) PROGRAM

The University's Identity Theft Prevention Program (Red Flag) applies to all Authorized Users accessing the University's Technology Resources regardless of their capacity, role or

function including, but not limited to, students, faculty, staff, third party contractors, visitors, guests, consultants, and employees fulfilling temporary or part-time roles.

In compliance with the Red Flag Rules of the Federal Trade Commission (FTC) implementing the Fair and Accurate Credit Transactions Act of 2003 (FACTA), University has adopted this Identity Theft Prevention Program ("Program") to detect, prevent, and mitigate Identify Theft in connection with the opening of a Covered Account or any existing Covered Account. The Program is further intended to help protect students, faculty, staff, and other constituents and the University from damages related to the fraudulent activity of Identity Theft.

A. Identity Theft Program

In accordance with the Red Flags Rule, the University's Identity Theft Prevention Program includes reasonable procedures to:

1. Identify relevant Red Flags for new and existing Covered Accounts and incorporate them into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks or to the safety and soundness of the student from Identity Theft.

B. Identification of Red Flags

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The University identifies the following Red Flags in each of the listed categories:

1. Notifications and Warnings from Credit Reporting Agencies

- Report of fraud accompanying a credit report
- Notice or report from a credit agency of a credit freeze on an applicant
- Notice or report from a credit agency of an active duty alert for an applicant
- Receipt of a notice of address discrepancy in response to a credit report request
- Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity

2. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic
- Identification document or card on which a person's photo or physical description is not consistent with the person presenting the document
- Other document with information that is not consistent with existing, readily available student information

- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled

3. Suspicious Personal Identifying Information

- PII presented that is inconsistent with other information the student provides (ex. inconsistent birth dates, lack or correlation between Social Security Number and date of birth)
- PII presented that is inconsistent with other sources of information (ex. an address not matching an address on a loan application)
- PII presented that is the same as information shown on other applications that were found to be fraudulent
- PII presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address)
- Social security number presented that is the same as one given by another student
- An address or phone number presented is the same as that of another person
- A person fails to provide complete personal PII on an application when reminded to do so
- A person's PII is not consistent with the information that is on file for the student

4. Suspicious Account Activity or Unusual Use of Account

- Change of address for an account followed by a request to change a student's name
- Payments stop on an otherwise consistently up-to-date account
- Account used in a way that is not consistent with prior use (large transfer of a credit balance to a One Card account)
- Mail sent to a student that is consistently returned as undeliverable although transactions continue to be conducted with the student
- Notice to the University (from the student) that the student is not receiving mail sent by the University;
- Notice to the University that an account has unauthorized activity
- A breach in the University's computer security system
- Any unauthorized access to or use of student account information

5. Alerts from Other Red Flags

Notice to the University from a student, identity theft victim, law enforcement, or other person that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft.

C. Detecting Red Flags

1. *New Accounts*: In order to detect any of the Red Flags identified above associated with the opening of a new Covered Account, University personnel will take the following steps to obtain and verify the identity of the person opening the account: (a) require certain identifying information such as name, date of birth, academic records, home address or other identification; (b) verify the individual's identity at time of issuance of identification cards (review of driver's license or other government-issued photo identification); and (c) independently contact the affected individual if appropriate.

2. *Existing Accounts*: In order to detect any of the Red Flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account: (a) verify the identification of students if they request information (in person, via telephone, via facsimile, via email); (b) verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and (c) verify changes in banking information given for billing and payment purposes.

3. *Consumer ("Credit") Report Requests*: In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel will assist in identifying address discrepancies by: (a) requiring written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and (b) in the event that notice of an address discrepancy is received, verifying that the credit report pertains to the applicant for whom the requested report was made and reporting to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

D. Preventing and Mitigating Identify Theft

All potentially fraudulent activity must be reported to the Program Administrator (see Section E below), who will work with relevant personnel to gather all related documentation and determine whether the attempted transaction was fraudulent or authentic and will respond appropriately. If it is determined by the Program Administrator that the attempted transaction was authentic, appropriate responses may include, but are not limited to:

- Terminating a transaction
- Contacting the customer
- Changing passwords, security codes, or other security devices that permit access to a Covered Account
- Not opening a Covered Account; closing an existing Covered Account
- Notifying and cooperating with appropriate law enforcement, and/or
- Determining that no response is warranted under the particular circumstances

E. Program Administration

Oversight: Responsibility for developing, implementing and updating this Program lies with the Vice President for Finance and Treasurer or the CIO who has been designated as the

Program Administrator. The Program Administrator will be responsible for ensuring appropriate training of University staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

Staff Training and Reports: University staff responsible for implementing the Program will be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. Appropriate University employees will be trained, as necessary, to effectively implement the Program. University employees are also expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, University staff responsible for the development, implementation, and administration of the Program will report to the Program Administrator on compliance with this Program. The report shall address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

Service Provider Arrangements: In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, it will require, by contract, that the service provider have appropriate policies and procedures in place to detect Red Flags and contractually agree to report Red Flags to the Program Administrator or the University employee with primary oversight of the service provider relationship.

Non-disclosure of Specific Practices: For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be shared with other employees or the public. The Program Administrator shall inform those employees with a need to know the information of those documents or specific practices which shall be maintained in a confidential manner.

Program Updates: The Program Administrator will periodically review and update this Program to reflect changes in risks to students and the soundness of the University from Identity Theft. In doing so, the Program Administrator will consider the University's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program.

R. WIRELESS NETWORK

1. The purpose of this Section is to secure and protect the information assets owned by University. University provides computer devices, networks, and other electronic information systems to

meet its mission, goals, and objectives. University grants access to these resources according to an individual's role and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This policy specifies the conditions that wireless infrastructure devices must satisfy in order to connect to the University network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by Information Technology Services are approved for connection to the University network.

2. This section addresses the requirements of Wireless deployments, Wireless network usage, and Wireless airspace usage. All employees, students, guests, contractors, consultants, temporary workers, and others who use the University network, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of University, must adhere to this section.

This section applies to all wireless infrastructure devices that connect to the University network or reside at an University owned, leased or rented site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

3. Wireless Deployments

Standards supported:

- 2.4 GHz and 5GHz broadcast frequencies are supported
- IEEE 802.1X is the authentication standard. Additional security procedures may be applied as needed

4. Wireless Service Considerations

Wireless networking has bandwidth limitations compared to the wired network. Applications that require large amounts of bandwidth, or are sensitive to changes in signal quality and strength may not be appropriate for wireless access. Some protocols and services will not effectively work in, or may be inappropriate for, a wireless environment.

5. Wireless IP Addresses

DHCP is the standard addressing method for the University networks. Wireless is a dynamic service. Due to the dynamic nature of wireless, IP space serving the campus will change over time due to capacity re-engineering.

Restrictions: all deployments of wireless infrastructure must be installed and maintained by IT. Installing departmental or do-it-yourself wireless access points is prohibited to avoid possible interference with the University wireless network, unnecessary impact to the wired network and to minimize undue security risks to the University.

Additionally, in areas where centrally managed wireless networking is available any pre-existing locally managed access points must be removed. Use of the wireless network is subject to the established

policies for use of the University campus network services. Only devices authenticated via University account credentials may access network resources on the University network that are not Internet facing.

6. Wireless Usage

Authenticated Access - Role-based access to the network shall be established using the user's University account credentials. All wireless data transactions shall be encrypted and secured by the protocols listed in the Supported Standards section above. Services allowed through the wireless network should be substantially identical to those for wired access. Role based users will be limited to those same services they are permitted to access via wired network controls. Three wireless networks are available on the University campus:

- AUWIRELESS = Staff/Faculty network, routable to wired faculty/staff network
- AUWIFI = Student Network (Not routable to faculty/staff network. Students are required to be registered with the Network access control system to insure that they have anti-virus software, appropriate operating system updates and security patches. Students cannot get on AUWIRELESS. It is a 64character wpa2 code)
- AUguest = Guest network, can only access the internet with limited bandwidth

7. Wireless Airspace

To provide wireless access, the radio frequency airspace of the campus serves as the transport medium for this technology. Wireless networks operate on the campus shared and finite airspace spectrum. Therefore, IT will regulate and manage this airspace centrally to ensure its fair and efficient allocation and to prevent collision, interference, unauthorized intrusion and failure. In addition, central management will facilitate the adoption of new features. IT will approach the shared use of the wireless radio frequencies in the same way that it manages the shared use of the wired network. Specific issues pertaining to wireless network devices are outlined below:

a. All access points will be installed and configured in such a way as to comply with all security features of the wireless network, including restrictions to provide connections only to those users who are entitled to access.

b. The University reserves the right to remove, disconnect or electronically limit any access point not installed and configured by IT personnel or specifically covered by prior written agreement and/or arrangement with IT.

c. Only users affiliated with University are authorized to use wireless networking on campus. To help protect these affiliated users from unauthorized access to their computer resources, IT will implement data encryption and authentication security measures that must be followed by all users. These measures require the use of specific wireless LAN product types and are designed to meet emerging wireless encryption and security standards.

S. IT/ATS SUPPORTED RESOURCES

This section relates to faculty, staff, and students who utilize University purchased IT/ATS resources. The purpose of this section is to identify what IT/ATS resources are supported for official use at University. This includes hardware and software resources.

IT/ATS will maintain a list of devices, systems and software supported by IT. This list can be found through the Technology section of MyArcadia (University intranet).

Resources on the list are reviewed continually and adjusted when appropriate. A representative from IT/ATS must be consulted in order to add resources to these lists. IT/ATS will decide whether or not a resource is capable of being supported. In cases where a resource may not be supportable, IT/ATS may recommend that a resource is purchased with additional vendor or third party support. If third party support is recommended and not purchased IT/ATS will not be able to support that resource.

1. **Academic Resources** *(ex. Classroom technology, Instructional software, etc.)*

If you have a suggested academic resource to be added to the supported list, please forward your request to ats@arcadia.edu and it will be reviewed by the Academic Technology Services Advisory Committee.

2. **Administrative Resources** *(ex. Administrative software, conference rooms, office technologies, servers, network infrastructure etc.)*

If you have a suggested administrative resource to be added to the supported list, please forward your request to helpdesk@arcadia.edu and it will be reviewed by CIO.

The University Acceptable Use Policy must be followed at all times when using any University purchased equipment.

T. DATA ACCESS CONTROL

This section is applicable to all electronic information for which the University is the custodian. The purpose of this section is to classify data based on the concept of 'need to know'. This phrase means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect University information from unauthorized use, disclosure, modification, and deletion.

1. Employee Responsibility

All University employees who come into contact with sensitive University internal information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily business activities. Sensitive information is either Confidential or Restricted information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for the University in classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

2. Information Classification

a. Restricted - This classification applies to the most sensitive business information that is intended for use strictly within University. Its unauthorized disclosure could seriously and adversely impact University, its customers and its business partners.

b. Confidential - This classification applies to less-sensitive business information that is intended for use within University. Its unauthorized disclosure could adversely impact University or its customers, business partners, or employees.

c. Public - This classification applies to information that has been approved by University management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

3. Data Owners

All electronic information managed by the University must have a designated owner. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the University management team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

Data owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. University must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

U. ACQUISITION AND DISPOSAL OF TECHNOLOGY RESOURCES

This Acquisition and Disposal of Technology Resources section applies to all members of the University community. IT is responsible for the full lifecycle of Technology Resources including their acquisition and disposal. The purpose of this section is to prescribe the methods by which Technology Resources are acquired and disposed of at University. The University technology infrastructure is a highly interconnected ecosystem that includes electronic and paper systems, software, equipment, licenses, information, policies, and procedures. It must be carefully architected, and methodically expanded, scaled back, or enhanced in accordance with this Policy.

1. Acquisition

All Technology Resources will be acquired and/or allocated through the change management process set forth below. Members of the University community wishing to acquire Technology Resources by purchasing, borrowing, renting, contracting, subscription, or donation must adhere to these procedures.

a. Assessment The IT Advisory Committee constantly assesses the University's Technology Resources and considers changes as necessary. Steps leading up to and involving the change management process include the following:

- Request for change (i.e., new version of software, bug fix, hardware purchases, etc.) triggers the need for the change management process;
- Steps required to make the change are identified by the IT Advisory Committee in consultation with the CIO;
- Initial risk and impact on the University is determined and documented;
- A test plan is created;
- A date of implementation is estimated based on who is affected and how long it will take to complete the change;
- Appropriate approval is obtained (see below).

Requests for additional reviews of technology resources must be submitted to the CIO, who chairs the IT Advisory Committee.

b. Approval and Schedule

(i) Low Impact Changes: Low impact changes include installation of new resources or reconfiguration of existing resources where the procedure impacts only a minimal amount of University departments and can be reversed easily and quickly with minimum downtime. Low impact changes must be recommended by the IT Advisory Committee and approved by the appropriate area vice president to ensure that the proposed change will function properly with the University's network configuration and that there is no duplication in equipment or services. Once approval is obtained, all resource-related purchase requests (including hardware and software related purchases) must adhere to current University purchasing procedures. Low impact changes can be made as soon as the change control request is approved.

(ii) Medium and High Impact Changes: Medium and High impact, strategic changes include installation of new resources or reconfiguration of existing resources that affect the entire University. The changes may also require significant down time. The IT Advisory Committee must initially recommend the change request to ensure that the proposed change twill function properly with the University's network configuration and that there is no duplication in equipment or services. The request then must be presented to the Senior Administration and then the President for final approval. Once final approval from the President of the University is obtained, all resource related purchase requests (including hardware and software related purchases) must adhere to current University purchasing procedures. Changes can be made on the agreed upon date after approval as described above, proper notification, and testing.

(iii) Emergency Changes: There are situations where, in order to support the continuity of University operations, an emergency change will be required. An Emergency includes any change, which if not implemented, would greatly impede University productivity or cause unacceptable additional costs. All emergency changes require the approval of the President after consultation with the CIO.

(iv) Notification Requirements: Upon approval of the change as applicable, notification of the change is required as part of the change management process. The individuals to be notified will depend on: the department affected by the change, the level of risk involved, and the amount of downtime needed to make the change. Outside of emergency changes, the

timing of notifications will be reasonable to allow for a response and any alternate plans that need to be made by those affected by the changes.

2. Disposal

Technology Resources will be replaced, repaired, improved, or disposed of by IT. All resources that are no longer being used productively for University business must be returned to IT for reallocation, repair, or disposal. Members of the University community may not directly give, lend, rent, donate, or dispose of Technology Resources.

When Institutional Data is no longer needed it must be methodically and securely rendered inaccessible or unusable in local or hosted systems or data storage (such as servers, desktop and laptop disks, mobile devices storage, removable storage such as memory sticks, CDs and DVDs, and backup media). IT will coordinate the secure handling of Institutional Data that is no longer needed.

V. INSTITUTIONAL DATA SECURITY

This University's Information Data Security section applies to all Authorized Users who have access to Institutional Data regardless of their capacity, role or function including, but not limited to, students, faculty, staff, third party contractors, visitors (guests), consultants, and employees fulfilling temporary or part-time roles. The purpose of this section is to provide direction for the information security program in support of the mission of the University and to ensure compliance with laws and regulatory requirements. The section establishes the governance structure for information security throughout the University, and expresses management expectations and role-based responsibility.

Authorized Users Technology Resources have a responsibility to properly use such resources, protect Institutional Data, and to respect the rights of others in accordance with this section, as well as the University's Acceptable Use Policy and Section Q (Identity Theft Prevention Program (Red Flag Rule)) and Section W (Protection of Consumer Financial Information).

1. Official Technology Resource Systems and Services

To assist the University in maintaining compliance with applicable data integrity, privacy and security policies, procedures, standards, and legal requirements, all members of the University community are required to conduct all official University business utilizing University' s official Technology Resource systems and services.

2. Location of Electronic Institutional Data

Institutional Data is stored on central servers and maintained by remote hosting service providers, as well as on individual computers and electronic devices, including but not limited to, laptops, desktops, and Mobile Devices. Such a diverse networked environment poses risks to the security of Institutional Data. Protecting Institutional Data is a shared responsibility between IT and Authorized Users of that information.

3. Designation of a Data Steward in Each Department

Each administrative department shall designate a data steward, typically the head of the department, who is responsible for Institutional Data and specific administration applications in the individual's functional area. The data steward's specific responsibilities include:

- Review and approval of all requests for access to and updating of Institutional Data and all applications that support Institutional Data,
- Ensuring that departmental use of Institutional Data is consistent with this Policy and other related University policies, including the University's FERPA policy and Section Q (Protection of Consumer Financial Information),
- Ensuring that all individuals who are given access to PII are instructed about its confidential nature,
- Ensuring that administrative systems which are not managed by IT but that store Institutional Data are secured and protected from unauthorized use, improper disclosure, accidental alteration, and that such systems are properly maintained and backed up; and
- The facilitation of administrative access for the appropriate users through training new users and collaboration with the CIO.

Although some of the responsibilities of the data steward may be delegated to others in the functional area, the data steward continues to have overall accountability for the use and security of the Institutional Data.

4. Administrative Access

a. Obtaining Administrative Access

Requests for access to Institutional Data for an Authorized User must be submitted electronically or in writing in the form of a security request form to the CIO. Only the requested and approved access that is specific to an Authorized User's responsibilities will be granted. The following procedure must be followed to grant administrative access to new Authorized Users:

- The relevant data steward must review and explain this section to the Authorized User;
- The IT staff (designated by the CIO) creates the login and assigns the level of access to the new Authorized User; and
- The data steward trains the new Authorized User to comply with this section.

b. Appropriate Use of Administrative Access

Administrative access may only be used for official University business and then only on a "need to know" basis. Such access may only be engaged using the tools and means prescribed by IT, for the stated purpose. Administrative access should be consistent with a user's role or job responsibilities as prescribed by the appropriate data steward. When a user's role or job responsibilities change, administrative access must be appropriately updated or removed. In situations where it is unclear whether a particular action is appropriate and within the scope of current job responsibility, the situation should be discussed with the appropriate data steward or the CIO.

c. Inappropriate Use of Administrative Access

In addition to those activities deemed inappropriate in the University Acceptable Use Policy, FERPA Policy, Section Q (Identity Theft Prevention Program (Red Flag Rule)), and Section W (Protection of Consumer Financial Information), the following constitutes inappropriate use of administrative access to AU Technology Resources unless documented and approved by the CIO:

- Circumventing user access controls or any other formal University security controls;
- Circumventing bandwidth limits or any other formal University computing controls
- Circumventing formal account activation/suspension procedures;
- Circumventing formal account access change request procedures; and
- Circumventing any other University policy or procedure.

The following constitutes inappropriate use of administrative access to AU computing resources under any circumstances, regardless of whether the use has been approved:

- Unauthorized access to PII;
- Exposing or otherwise disclosing PII to unauthorized persons; and
- Any use or access of Institutional Data outside the scope of administrative access rights granted by the IT Administrator, including using access to Institutional Data to satisfy personal curiosity about an individual, system, practice, or other type of entity.

d. Termination or Change of Status of Users

Administrative department heads and academic department chairs are responsible for informing Human Resources and the appropriate vice president of an employee's change in status or termination. Changes in status may include leaves of absence, significant changes in positional responsibilities or transfer to another department or division. Human Resources is responsible for making a record of the change in status and notifying the appropriate organizations, including IT. The CIO is then responsible for delegating appropriate IT personnel to modify or terminate the user's administrative access.

e. Additional Access Controls

- Where practicable, the University separates the duties of Authorized Users to reduce the risk of malevolent activity without collusion.
- The University employs the principle of least privilege, including for specific security functions and privileged accounts.
- The University uses non-privileged accounts or roles when accessing non-security functions.
- The University prevents non-privileged users from executing privileged functions and audits the execution of such functions.
- The University limits unsuccessful logon attempts.

- The University provides privacy and security notices as necessary.
- The University uses session lock with pattern-hiding displays to prevent access/viewing of data after a period of inactivity.
- The University terminates (automatically) an Authorized User's session after a defined condition.
- The University monitors and controls remote access sessions.
- The University employs cryptographic mechanisms to protect the confidentiality of remote access sessions.
- The University routes remote access via managed access control points.
- The University authorizes remote execution of privileged commands and remote access to security-relevant information.
- The University authorizes wireless access prior to allowing such connections.
- The University protects wireless access using authentication and encryption.
- The University controls connection of Mobile Devices to its Technology Resource systems.
- The University encrypt Institutional Data on Mobile Devices.
- The University verifies and controls/limits connections to and use of external Technology Resource systems.
- The University limits the use of organizational portable storage devices on external Technology Resource systems.
- The University controls information posted or processed on publicly accessible Technology Resource systems.

5. Data: Extraction of Institutional Data

Extraction/downloading of Institutional Data for processing on systems, including desktop PCs, laptops, Mobile Devices, or any physical or electronic storage medium, other than networks and systems physically maintained by IT, shall only be done if the confidentiality, integrity, and accuracy of the institutional data can be ensured and the physical, technical and administrative safeguards outlined in Section Q (Identity Theft Prevention Program (Red Flag Rule)) and Section W (Protection of Consumer Financial Information) can be maintained.

6. Periodic Review of Data Security Configurations

On a periodic basis, the appropriate data steward reviews Users' access to Institutional Data in University administrative data systems.

7. Audit and Accountability

IT creates, protects, and retains audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate activity. Moreover, IT ensures that the actions of Authorized Users can be

uniquely traced to those users so they can be held accountable for their actions. In addition, IT performs the following tasks on a regular basis:

- Reviews and updates audited events,
- Issues alerts in the event of an audit process failure,
- Correlates audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity,
- Provides audit reduction and report generation to support on-demand analysis and reporting,
- Provides an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records,
- Protect audit information and audit tools from unauthorized access, modification, and deletion, and
- Limits management of audit functionality to a subset of Authorized Users.

8. Reporting Data Security Breaches

If any user reasonably believes that any violation of this policy or breach or potential breach of any institutional data may have occurred, the user is required to immediately report to the appropriate data steward or CIO of the University. Thereafter, Section N, (Security Incident Response), will be implemented.

9. Baseline Requirements and Responsibilities

a. User Requirements

1. Configuration: Computers and other devices housing Institutional Data must be set up in accordance with the applicable University security guidelines and standards. Such security guidelines and principles are outlined in this section below. Computers and devices housing Institutional Data and controlled or operated by a third party user must, at a minimum, be subject to the same security guidelines and principles.

IT establishes and maintains baseline configurations and inventories of the University Technology Resource systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. In addition, IT establishes and enforces security configuration settings for information technology products employed in the Technology Resource system. Specifically, IT performs the following tasks on a regular basis:

- IT tracks, reviews, approves/disapproves, and audits changes to Technology Resource system,
- IT analyzes the security impact of changes prior to implementation,
- IT, in collaboration with department data stewards, defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the Technology Resource system,

- IT employs the principle of least functionality by configuring the Technology Resource system to provide only essential capabilities,
- IT restricts, disables, and prevents the use of nonessential programs, functions, ports, protocols, and services, and
- IT applies deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- IT controls and monitors user-installed software.

2. Authentication: Administrative access and any access to PII must be authenticated (e.g. by using a strong and complex password) with file access privileges differentiated by user. Administrator access passwords should be exceptionally strong and all PCs, laptops, and Mobile Devices must be password protected in accordance with the section M (see also Section N Security Incident Response). In addition, IT performs the following authentication tasks on a regular basis:

- IT uses multifactor to privileged accounts and for network access to non-privileged accounts,
- IT employs replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts,
- IT prevents reuse of identifiers for a defined period,
- IT disables identifiers after a defined period of inactivity,
- IT enforces a minimum password complexity and change of characters when new passwords are created,
- IT prohibits password reuse for a specified number of generations,
- IT permits temporary password use for system logons with an immediate change to a permanent password,
- IT stores and transmits only encrypted representation of passwords, and
- IT obscures feedback of authentication information.

3. Encryption: For PII that is sent across the Internet (external to the University's network) or other open network such as a wireless connection, both the authentication data (e.g. a user id and password) and the data itself must be encrypted. Encryption of PII stored on laptop computers or other portable devices is required. Such data may only be stored with IT permission. An offsite plaintext backup version in a secure location is recommended to protect against lost encryption keys. University's wired network is not considered an open network. IT provides information to enable users to comply with this provision if they are sending or receiving PII on a network that is external to University's network.

4. Personnel Security: Human Resources screens employees at the time of hire prior to obtaining administrative access. In addition, the University ensures that Institutional Data and Technology Resource systems containing Institutional Data

are protected during and after personnel actions such as terminations and transfers by revoking user access (see Section V 4d above).

5. Media[2] Protection: University departments protect (i.e., physically control and securely store) information system media containing Institutional Data, both paper and digital. The University limits access to Institutional Data on information system media to authorized users. Moreover, the University sanitizes or destroys information system media containing Institutional Data before disposal or release for reuse. More specifically, the University takes the following actions with respect to media protection:

- For Institutional Data that is stored in paper form, Authorized Users must properly secure the data to avoid loss, theft or other misappropriation. Such forms of physical security include: proper filing of the Institutional Data in secure data storage compartments and using appropriate enclosures and labeling for the physical transmittal of Institutional Data within AU so that only Authorized Users view the information.
- IT controls access to media containing Institutional Data and maintains accountability for media during transport outside of controlled areas.
- IT implements cryptographic mechanisms to protect the confidentiality of Institutional Data stored on digital media during transport unless otherwise protected by alternative physical safeguards.
- IT controls the use of removable media on information system components.
- IT prohibits the use of portable storage devices when such devices have no identifiable owner.
- IT protects the confidentiality of backup Institutional Data at storage locations.

6. Anti-virus technology: Desktop and laptop computers must have anti-virus software or filters installed and updated daily (automatic updates recommended) according to the guidelines provided by IT. In addition, other Windows computers, including servers, must have anti-virus software installed and updated daily.

7. Firewall or filtering: A software firewall, hardware firewall, or other network filtering (e.g. port or IP address filtering) technology must be used to limit network access to the device storing PII.

8. University Responsibilities:

The University has primary responsibility for the following and has delegated most operational responsibilities to the CIO:

[2] Media - Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

- **Technical support required**: Computers and other devices must be either continuously managed or reviewed on an ongoing basis for appropriate security measures according to the guidelines provided by IT. These reviews must include adherence to baseline security requirements outlined in this policy and other AU data security policies as well as additional strategies for protecting the information.

- **Staffing level**: All departments and units that manage users must have appropriately supervised professional technical support staffing sufficient to maintain information security. The staffing level should be appropriate to the environment, i.e. the amount and type of institutional data, for which they are responsible and the level of risk. Collaboration with the CIO will be necessary to determine the appropriate level of staffing.

i. Security Assessment: IT periodically assesses the security controls in University information systems to determine if the controls are effective in their application, as well as develops and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in information systems. In addition, IT monitors information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

j. Maintenance and Patching: Security vulnerabilities are regularly found and publicized for software. Regular patching, installation of newer versions, and other maintenance is performed by IT to protect Institutional Data. Automatic settings or centralized updating of security patches is recommended for most computers. In addition, IT regularly performs the following maintenance tasks:

- Ensures equipment removed for off-site maintenance is sanitized of any Institutional Data.
- IT checks media containing diagnostic and test programs for malicious code before the media are used in a University information system.
- IT requires multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminates such connections when nonlocal maintenance is complete.
- IT supervises the maintenance activities of maintenance personnel without required access authorization.

k. Physical Access: Physical access to computers and Mobile Devices must be restricted as much as possible. Escort visitors and monitor visitor activity. Ensure that you lock access to your devices when you are not using them. Lock your office if feasible when you are out and secure Mobile Devices in a locked desk draw. When traveling keep your devices with you and in sight at all times. At a hotel room secure your mobile technology in the room safe.

l. System and Communications Protections: The University monitors, controls, and protects organizational communications (i.e., information transmitted or received by the University's information systems) at the external boundaries and key internal boundaries

of the University's information systems. In addition it employs architectural designs, software development techniques, and systems engineering principles that promote effective information security within the information systems. Specifically, IT implements the following system and communication protections:

- IT separates user functionality from information system management functionality.
- IT implements sub-networks for publicly accessible system components that are physically or logically separated from internal networks.
- IT denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).
- IT prevents remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.
- IT implements cryptographic mechanisms to prevent unauthorized disclosure of Institutional Data during transmission unless otherwise protected by alternative physical safeguards.
- IT terminates network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
- IT establishes and manages cryptographic keys for cryptography employed in the information system.
- IT employs FIPS-validated cryptography when used to protect the confidentiality of Institutional Data.
- IT prohibits remote activation of collaborative computing devices and provides indication of devices in use to users present at the device.
- IT controls and monitors the use of mobile code.
- IT control and monitors the use of Voice over Internet Protocol (VoIP) technologies.
- IT protects the authenticity of communications sessions.
- IT protects the confidentiality of Institutional Data at rest.

a. **Security event logging**: Host security log files must be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event (at least 90 days of logs).

b. **Reporting critical servers**: Servers storing Institutional Data (including PII), including servers hosted by third parties, must be identified and scanned regularly with vulnerability testing software.

c. **Backups**: Periodic backup copies of software and data must be made, tested, and stored securely (not in staff cars, homes, etc.). The physical security of the removable media must be maintained and plans made to allow recovery from unexpected problems.

d. **Disposal of data and equipment**: A "secure deletion" program must be used to erase data from hard disks and media prior to transfer or disposal of hardware (See secure deletion). Permanent media (e.g., CD's, media storage devices, etc.) must be physically destroyed.

e. **Limit services**: Services available on computers or other devices must be as limited as possible. Web server, ftp server, mail server, peer to peer, and anonymous file sharing software can significantly raise the security risk to Institutional Data (including PII). Unless a high level of expertise is available and these services are closely monitored at all times, this higher risk software should not be installed.

f. **Training**: Both new and existing employees must complete training provided by the University on data security practices.

g. **Additional actions**: One or more of the following additional actions should be used to further protect PII, depending upon the situation and requirements:

   i. Encryption of all PII that is stored on any AU server or network or host server or network (with a clear-text version on a removable medium stored in a safe place); and

   ii. Separate any PII from other Institutional Data and store independently (e.g., on a non-networked device).

W. PROTECTION OF CONSUMER FINANCIAL INFORMATION

The University's Protection on Consumer Financial Information section applies to all Authorized Users who have access to Personally Identifiable Information (PII) regardless of their capacity, role or function including, but not limited to, students, faculty, staff, third party contractors, visitors (guests), consultants, and employees fulfilling temporary or part-time roles.

In compliance with the Gramm-Leach-Bliley (GLB) Act, University protects the private PII of consumers, students, and employees. The University's policy is to identify and safeguard this information with the appropriate procedures to insure compliance with the GLB Act. The University will manage PII in accordance with all applicable state and federal guidelines relating to the use, disclosure and retention of such information.

1. Information Security Plan

The GLB Act mandates that University appoint an Information Security Plan Coordinator; conduct a risk assessment of likely security and privacy risks; institute a training program for all employees who have access to PII; oversee service providers and contracts; and evaluate and adjust the Information Security Plan periodically.

2. Information Security Plan Coordinator

In order to comply with GLB, University has designated the CIO to act as the Information Security Plan Coordinator for the GLB Act. The CIO works closely with IT staff, as well as all relevant academic and administrative departments and divisions throughout the University.

3. Risk Assessment and Safeguards

The CIO works with all relevant areas of the University to identify potential and actual risks to security and privacy of PII. Each department head, or a designee, will conduct an annual data security review, with guidance from the CIO. Department heads will be asked to identify any employees in their respective areas that work with PII data and information. In addition, under the guidance of the CIO, the University will conduct an annual review of procedures, incidents of actual or attempted attacks to unlawfully obtain PII, and responses, and will publish all relevant materials to applicable employees except in those cases where publication may likely lead to breaches of security or privacy. Publication of these materials is for the purpose of educating the University community on network security and privacy issues.

In order to protect the security and integrity of the University's network and information systems and its data, the University maintains a registry of all computers attached to University network and information systems. IT staff also ensures that all electronic PII is encrypted in transit and that the central databases and systems are strongly protected from security risks.

In addition, IT staff utilizes event logs that are built into the system to monitor any actual or attempted attacks. IT also provides network security and user account security that prevents actual or attempted unauthorized access to covered PII data or information, as well implements those other safeguards and actions set forth in the University's Institutional Data Security Policy.

Social security numbers are considered PII under both GLB and FERPA. By necessity, student social security numbers still remain in the University's student information system. The University conducts regular assessments to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. These assessments apply to University employees as well as subcontractors.

Finally, the CIO periodically reviews University Technology Resource security, disaster recovery program, and data-retention policies.

4. Securing Information

The University has several formal policies and procedures that address information security of PII as required by the GLB Act as well as consequences for failing to maintain the confidentiality of certain information, including:

- FERPA Policy
- Section Q the Identity Theft Prevention Program (Red Flag Rule)
- Section W Protection of Consumer Financial Information
- Section N Security Incident Response

For ease of reference, below is a non-exhaustive summary of some key safeguards, controls, procedures, and practices utilized by the University:

- Maintaining physical security by locking rooms and file cabinets where PII is stored. Ensuring windows are locked and using safes when practicable for especially sensitive PII data such as credit card information, checks, and currency,

- Maintaining adequate key or access card control and limiting access to sensitive areas to those individuals with appropriate clearance who require access to those areas as result of their job,
- Securing the personal work area to discourage casual viewing of PII data by unauthorized individuals,
- Using and frequently changing passwords to access automated systems that process PII,
- Protecting the confidentiality of passwords by not sharing or posting such passwords;
- Using firewalls and encrypting information when feasible,
- Prohibiting the use of storage devices (e.g., laptops, external drives, etc.) to transport PII of consumers, students, and employees. Access to this information remotely is done only by using the VPN provided by the University,
- Protecting the confidentiality of electronic PII that might be accessed remotely either from home or in travel status. Under no circumstances should safeguarded information be "viewable" by unauthorized individuals,
- Referring calls and mail requesting customer information to those individuals who are familiar with safeguarding PII,
- Shredding and erasing customer PII when no longer needed,
- Encouraging employees to report suspicious activity to supervisors, and
- Ensuring that agreements with third-party contractors contain safeguarding provisions and monitoring those agreements to oversee compliance.

5. Oversight of Service Providers and Contracts

The GLB Act requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered PII data and information. The CIO will contact all identified covered contractors requesting assurances of GLB Act compliance.

6. Employees Training and Education

While department heads are ultimately responsible for ensuring compliance with the University's information security practices, IT will work in cooperation with Human Resources to develop training and education programs for all employees who have access to PII.

7. Evaluations and Revision

The GLB Act mandates that this Information Security Plan be subject to periodic review and adjustment. The most frequent of these reviews will occur within IT. Processes in other relevant offices such as data access procedures and the training program also undergo regular review. The plan itself will be reevaluated regularly in order to assure ongoing compliance with existing and future laws and regulations.

X. SOCIAL MEDIA

This section applies to all members of the University community.

The purpose of this section is to establish the University's procedures for creating and approving content pertaining to University (including the University's schools, departments, divisions, offices, centers, programs, series, etc.) on any publicly available Website or social media platforms. In addition, guidelines are provided to the general campus community regarding personal use of social media.

The University's official presence on social media platforms is overseen by University Relations. Websites and/or accounts that purport to represent information as University (including the schools, departments, divisions, offices, centers, programs, series, etc.) on any publicly available Website or social media platforms must be approved by the appropriate area vice president and coordinated with University Relations.

Websites/providers or social media platforms that host unauthorized accounts using identification as University or its subdivisions, in name or image, including the University seal or its logos—will be contacted for immediate removal of accounts.

1. University Use of Social Media

The University supports the official use of social media to reach audiences important to the institution. This policy establishes the criteria and procedure for creating a University presence, account, or participation on external social media sites such as Facebook, LinkedIn, Twitter, YouTube, etc. on behalf of the University.

a. Approval of University Social Media Initiatives

The following criteria will be considered when there is a request to establish a University-hosted social media site or to participate in social media on behalf of the University:

- Whether or not the University's involvement can be carried out in such a manner that positively supports the institution's values, missions, and goals,
- Whether or not the engagement with the audience adds value to both the University and the audience,
- Whether or not the approach is as effective or efficient as other approaches that might be used (i.e. would an existing University social media initiative or the University Website accomplish the same goals),
- Whether or not the use of social media enables the University to offer services it might not otherwise be able to offer, and
- Whether or not sufficient resources exist to appropriately manage the interactions.

At least one University employee will be designated to monitor the medium, identify problems that emerge, take action when necessary, and ensure timeliness and accuracy of content.

Any use of University marks, such as logos and graphics, must comply with the University's identity guidelines.

b. Approval Process

The appropriate vice president or designee will approve a request for a University presence or participation on social media sites on behalf of the University.

Once approved, the request will be forwarded to University Relations for approval. If the presence or participation on social media sites involves a University athletic program, the request will be forwarded to the University Athletic Director.

The level of editorial control for a University presence or participation on social media sites will be identified and agreed upon with University communications or sports information, as applicable, during the approval process.

c. Updating and Monitoring Accounts

Pages should be updated on an ongoing basis to enable rapid response to any issues that may arise and to ensure an engaging, interesting environment for visitors. To be effective, pages must be dynamic and require consistent updating.

Employee use of approved social media on behalf of the University should be consistent with University policy, including but not limited to the University's identity guidelines and acceptable use, copyright, and student record policies. University communications or sports information, as applicable, are charged with the responsibility to monitor the University's social media initiatives, counsel those who represent the University online regarding University policy, and take action to restrict or remove an employee's ability to "publish" should efforts to correct the situation fail.

2. Personal Use of Social Media

a. University Employees

Personal use (e.g., when an employee uses social networking sites as part of the employee's personal life) of University electronic resources during business hours to access social networking sites or posting of blogs should be limited to incidental use. Incidental use should not interfere with an individual's performance of assigned job responsibilities or someone else's job performance or compromise the functionality of the campus network.

In using such sites or mediums, employees should refrain from presenting personal opinions in ways that imply endorsement by the University. If posted material may reasonably be construed as implying the support, endorsement, or opposition of the University with regard to any personal statements, including opinions or views on any issue, the material should be accompanied by an explicit statement that the individual is speaking for oneself and not as a representative of the University.

In addition, an employee's personal use of social media or electronic postings should be consistent with University policy. Examples of postings that are contrary to University policy include, but are not limited to the following:

- Unlawfully discriminatory or harassing behavior against a member of the University community,
- Posting of materials or information in violation of the University's confidentiality or student record policies or provisions protecting trade secrets contained in any University confidentiality agreement,
- Posting that unlawfully defaming or disparaging the University, its employees, students, or work product, or

- Non-approved use of the University's name or the posting of the University's seal, logo, trade and service mark, monograms, or images.

Employees are also cautioned not to post information, photos, or other items online that could reflect negatively on the University's mission.

In response to concerns or complaints or information provided by individuals, University administrators may look up profiles on social networking sites and may use the information in informal or formal disciplinary proceedings.

b. Students

University students must be concerned with any behavior that might reflect badly on themselves, their families, and University. Such behavior includes any activities conducted online.

Students are not restricted from using any online social networking site and/or digital platform. However, users must understand that any content they make public via social media is expected to follow acceptable social behaviors and also to comply with federal and state government laws and University policies, procedures, rules, and regulations. Because social networking sites are part of the public domain, students should make use of any available privacy settings, and as a general rule should avoid posting sensitive personal information such as a home address, phone number or birth date. Students should also be aware that inappropriate conduct online could negatively impact their personal, academic and professional lives if viewed by University personnel, employers, internship supervisors, scholarship committees or admissions committees. If inappropriate conduct is deemed a violation of any law or regulation, disciplinary and/or law enforcement action will be taken. Examples of misconduct include, but are not limited to, derogatory language about any member of the University community; demeaning statements about or threats to any third party; and incriminating photos or statements depicting hazing, sexual or gender-based discrimination, vandalism, stalking, underage drinking, or illegal drug use.

c. Student Athletes

Participation in intercollegiate athletics at University is a privilege, not a right. While the Athletic Department does not prohibit student-athlete use of online social network sites and/or digital platforms, it must be understood that the high standard of integrity expected of student-athletes on the field also extends to areas off the field, such as comments and postings made to Internet sites. The Athletic Department reserves the right to take action against currently enrolled student-athletes engaged in online behavior that violates National Collegiate Athletic Association (NCAA), Colonial States Athletic Conference (CSAC), University, the Athletic Department, or team policies, rules, and regulations. This action may include education, counseling, team suspension, termination from the team, reduction or non-renewal of any athletic scholarships, disciplinary sanctions or involvement of law enforcement agencies.

Y. UNIVERSITY WEB PRESENCE

This University Web Presence section applies to all members of the University community.

The purpose of this section is to establish authority, responsibilities, and actions that assure that University's presence on the World Wide Web supports and promotes the University's mission.

All aspects of the University's Web presence represent official communications from the University to the public and must adhere to University policies and standards regarding content, branding, and technical structure.

The University's conduct policies including all copyright rules and restriction on the use of written, graphical, video, and audio materials and data, and standards and requirements for acknowledgment of sources in academic work must be met in all aspects of the University's Web presence.

1. Official University Webpages and Other Electronic Publications

The official webpages of the University are defined as those pages that represent elements of the University above the school or department level. Such webpages and other electronic publications are official University publications and, accordingly, they must conform to University web graphic identity guidelines and meet the appropriate standards for accessibility by users with disabilities.

All official University webpage revisions and additions must be reviewed by [University Relations] or, if the site involves an athletic program, [Sports Information]. Once approved, the revision or addition will be published to the Internet by the University webmaster. [University Relations] or Sports Information, as applicable, will confirm that the proposed postings are consistent with University policies and guidelines, as well as local, state, and federal law. Before University policies are posted to the "official" University website, such policies must have been vetted and approved through the University's policy approval process.

2. College/School/Department Webpages

College, school and department webpages and other electronic publications are the equivalent of printed publications or official communication. They are official University publications. University web graphic identity guidelines are available through University Relations. Each college, school and department webpage must contain:

- The college/school/department name,
- An electronic mail address for the college/school/ department's webpage creator or administrator,
- The page's expiration date when appropriate,
- A link to the University's copyright and disclaimer policies, and
- A link to the University's home page.

A college/school/department creating its own electronic information may set additional requirements, such as the inclusion of the equal opportunity statement. A college/school/department may decide whether it is of benefit to link the individual electronic pages of their faculty, staff, or students to the college/school/department webpage.

Official college/school/department pages must be maintained with current and relevant information, and the page owner may designate page administrators to maintain the content on their behalf.

Official college/school/department pages and academic pages must meet the appropriate standards for accessibility by users with disabilities.

All college/school/department webpage revisions and additions are completed in conjunction with University Relations. The final draft of the webpage must be reviewed and approved by the appropriate vice president prior to being published to the internet by the University webmaster. University Relations will confirm the proposed postings are consistent with University policies and guidelines, as well as local, state, and federal law.

3. Athletic Department Webpage

The official website of University Athletics is: http://www.arcadiaknights.com/. Updating rosters, schedules, biographical information on athletes and coaches and posting releases to the website is the direct responsibility of University Athletic Director.

4. Faculty and Staff Webpages

Faculty and staff may create webpages that provide information relevant to that individual's role at University. The work on individual webpages represents the work of individual artists, scholars, and authors who created them, and they are not intended to represent University. As such, University bears no responsibility for the content of individual webpages.

Each individual page, cluster of linked pages, or other electronically published information will display by a browser:

- The individual's name,
- The individual's position or affiliation with the University,
- The individual's University electronic mail address, and
- A link to the University's copyright and disclaimer policies.

Page owners should assert copyright when they own it.

Complaints of alleged breaches of web authoring guidelines or the Acceptable Use Policy by faculty or staff will be discussed with the individual. If the complaint cannot be resolved through discussion with the individual, the matter will be referred to the dean or director of the department. If resolution is still not reached the sanctions defined in the Acceptable Use Policy will be enforced. In addition, the University reserves the right to terminate the faculty or staff member's website.

5. Student Webpages

Students may create webpages and other electronic publications that provide information relevant to their course of study or interests. The work on individual webpages and electronic publications represents the work of the individual students who created them, and they are not intended to represent University. As such, University bears no responsibility for the content of student webpages.

Each individual page, cluster of linked pages, or other electronically published information will display by a browser:

- The student's name,
- The fact that they are a student at University,
- The individual's University electronic mail address, and

- A link to the University's copyright and disclaimer policies.

Complaints of alleged breaches of web authoring guidelines or Acceptable Use Policy will be filed according to the code of student conduct. If it is determined that the page is in violation of University policy, the page owner will be asked to correct the problem. If the problems are not corrected the site will be removed from the server. In addition, the University reserves the right to terminate the student's website.

6. Student Clubs and Associations Webpages

Individuals may create webpages and other electronic publications that provide information relevant to University sanctioned clubs and associations. The information on individual webpages represents the work of the club/association, and is not intended to represent University. All pages must be approved by a faculty or staff sponsor prior to publication.

Each individual page, cluster of linked pages, or other electronically published information will display by a browser:

- The name of club or association,
- The name and University email address of the faculty sponsor,
- The University electronic mail address of the individual responsible for developing the content, and
- A link to the University's copyright and disclaimer policies.

Complaints of alleged breaches of web authoring guidelines or Acceptable Use Policy will be discussed with the faculty sponsor. If the sponsor agrees that the page is in violation, the sponsor will arrange to have the problem corrected. If the problems are not corrected the site will be removed from the server. In addition, the University reserves the right to terminate the club or association's website.

7. General Guidelines

The University respects the First Amendment of the Constitution of the United States and does not restrict the content of employee and student webpages beyond the restrictions of University policy, applicable law, and the general guidelines set forth below. University, however, reserves the right to remove from any University server a webpage that is found to be in violation of the law or University policies.

In addition to University policy and applicable law, the following guidelines also apply to receiving and maintaining a website account:

- PII or confidential student data such as grades or class-rosters must not be posted. For questions relating to the confidentiality of student records, refer to the University's FERPA Policy or contact the Registrar,
- The use of website space for promoting or advertising commercial goods or services; soliciting customers or investors; or selling and distributing goods or services is strictly prohibited,
- Websites may not be used as archive space for any files not directly related to the website. Outdated and/or unlinked files shall not be stored on the server,

- The assigned website storage space is to be used by the assignee and shall not be used for or by outside entities, and
- Links to resources outside of the University server must not violate University policies, the University's mission, or local, state or Federal law.

Each individual website shall include a disclaimer indicating that the views and opinions expressed on the site are those of the site developer or organization and are not those of the University.

The content of pages is the responsibility of the individual owner, including the responsibility for making sure that their pages follow the Acceptable Use Policy. If a complaint of copyright infringement is brought against the individual, the page(s) in question will be temporarily removed while the allegation is investigated.

It is the responsibility of any page owner leaving University to copy and remove any unofficial page material. This includes faculty members who have left University and are not officially on leave, staff members who have left, and students who are no longer enrolled.

Unless other arrangements have been made, unofficial pages will be removed three-months after an individual's employment termination or graduation date.

8. Support

The University's IT department will provide the following support for departments as they adopt these policies:

- Provide an unlimited amount of server space for official pages, and 10mg of web server space to each University faculty, staff and student for web development,
- Provide templates and branding guidelines for official pages, and
- Provide designated individuals with a contribute interface for all official pages.

Z. MANAGEMENT AND USE OF MOBILE DEVICES

This Management and Use of Mobile Devices section applies to all Authorized Users accessing Institutional Data via a Mobile Device, as well as to all users of Mobile Devices on University's campus or at University activities.

The purpose for this section is to outline the requirements and user expectations for reading and manipulating Institutional Data on Mobile Devices. These devices extend the security boundary of the campus, in that they allow for the transportation, storage, and manipulation of Institutional Data. This section is intended to outline mechanisms for safeguarding that information. In addition, this Policy outlines expectations with respect to the general use of privately owned s on the University campus or at University activities. All users of Mobile Devices are expected to comply with this Policy. The use of Mobile Devices is also subject to the University's Acceptable Use Policy and other applicable University policies.

The use of a Mobile Device to access Institutional Data must be accomplished via secure and encrypted means if the Mobile Device is not directly connected to the University Network. Unauthorized access to Institutional Data utilizing a Mobile Device is prohibited.

In addition, Users are prohibited from using Mobile Devices utilizing the University's network(s) to violate copyrights including, but not limited to, copyrighted music, movies, software and publications. Moreover, photographing or digitally recording individuals with any Mobile Device that has photographic or video capturing capabilities in areas such as bathrooms, locker rooms, or other areas where there is a reasonable expectation of privacy, and/or taking photographs or video of an individual against their will is prohibited. Electronic transmission via the University's network(s) of photographs or video of any person without the subject's express permission is also prohibited. Finally, Mobile Devices may not be used on campus to record conversations unless all parties to the conversation give their consent.

1. Device Precautions

The following security requirements govern the use of any Mobile Devices that are used on the University's network(s), regardless of whether or not the device was purchased or leased with University funds:

- Remote access to the University's nonpublic-facing systems will be protected via secure or encrypted protocols. Only those employees and contractors whose job duties require this level of access will be granted remote access,
- All Mobile Devices accessing the University's network(s) must be updated to the latest device operating system with the latest security patches and anti-virus software,
- All applications must be updated with the latest security patches,
- Users may not allow someone who is not authorized access to the University network to use their devices if the device has been used to store, access and/or process Institutional Data,
- All devices that have been used to store, access and/or process Institutional Data must delete the data stored on their devices immediately after the work with it is completed,
- All devices must be configured with a PIN, passcode, or password-enabled lock screen configured to activate at no more than 5 minutes of inactivity,
- All devices with built-in encryption capability must have the device's encryption enabled,
- All devices must have "remote wipe" enabled through a third party application or the manufacturer's website,
- All devices that have been used to store, access and/or process Institutional Data must be wiped to remove such data before they are transferred to someone else through sale or gifting,
- In the event that a device which has been used to store, access and/or process Institutional Data becomes lost, stolen or compromised, the owner must contact the Information Technology, and

- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the University's network(s).

2. Consent

Users of personally owned Mobile Devices may access information through the University's portal. In accessing the portal with a personal Mobile Device, the user understands and agrees that the University will not reimburse or otherwise compensate the user for any costs associated with accessing the University network with a personal Mobile Device. Such costs may include, but are not limited to, monthly call and data plans, long distance calling charges, additional data or roaming fees, charges for excess minutes or usage, equipment, surcharges and any applicable fees or taxes. The user also understands that he/she may be held liable for any criminal and/or civil penalties that may result from loss, theft or misuse of the Institutional Data accessed and/or stored on the Mobil Device.

Upon termination of affiliation with the University, users agree: (a) to immediately delete all Institutional Data stored on the device; and (b) to remove the University email account and Wi-Fi settings from the device. Failure to complete the above may result in the device being remote wiped by IT.

3. Initial Configuration

To ensure proper initial configuration of Mobile Devices, users should consult with Information Technology before purchasing a new device to verify its suitability for the University's network environment.

For allowed University-owned/leased devices, IT will configure the device to access the campus email and calendar resources. A brief orientation session on proper use of the device can be scheduled with IT.

For allowed personal devices, IT will provide written procedures for configuring devices to access campus resources. It is the responsibility of the owner to configure the device properly, and should they need assistance, contact their service provider for further assistance.

4. Support

For University-owned /leased Mobile Devices, users should contact the Help Desk for assistance. Information Technology will handle all technical issues on behalf of the University.

For allowed personal Mobile Devices, users should contact their service provider for troubleshooting assistance.

5. Student Use of Mobile Devices in the Classroom

Mobile Devices may not be used in a manner that causes disruption in the classroom or library. Moreover, University does not allow the use of such devices to photograph or video any classes without instructor permission. Abuse of devices with photographic or video capabilities for purposes of photographing test questions or materials is a violation of University's academic integrity policy.

6. Use of Electronic Devices in Vehicles

The University is committed to promoting highway safety by encouraging the safe use of Mobile Devices by its students, faculty, administrators, and staff while operating a vehicle on

campus or in the performance of University business or a University sanctioned activity. If a University student or employee needs to use a Mobile Device under these circumstances, the individual is strongly encouraged to find a proper parking space and park the car before using the device. Parking on the side of the road is not recommended, except in the case of a genuine emergency. Students, faculty, administrators, and staff are expected to comply with applicable state laws including those laws requiring the use of hands-free functions. Violations of this Policy may result in disciplinary action.

7. Risks/Liabilities/Disclaimers

While the University will take every precaution to prevent the user's personal data from being lost in the event it must remote wipe a device, it is the user's responsibility to take additional precautions, such as backing up notes, documents, application data, etc. The University reserves the right to disconnect devices or disable services form its network without notification.

Users are personally liable for all costs associated with a non-University issued Mobile Device and assumes full liability for risks including, but not limited to, the partial or complete loss of Institutional Data and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

AA. CLOUD COMPUTING

This Cloud Computing section applies to all Authorized Users of Technology Resources at University.

The purpose of this section is to establish the University's policy and procedures regarding the protection of Institutional Data placed into a Cloud Computing environment that is not directly controlled by the University.

Institutional Data may not reside within any cloud-computing environment unless University has entered into a legally binding agreement with the service provider to ensure that the data are protected and managed in accordance with standards and procedures required by law and acceptable to the IT office.

Institutional Data placed into a University authorized cloud environment must be encrypted in transit and encrypted at rest. Moreover, the cloud service provider's contract must indicate that they conform to all relevant federal, state and local laws and regulations. Finally, any Institutional Data residing within a cloud-computing environment must be retrievable by the University and not solely by the individual who placed the data in the cloud environment, and must conform to Section EE (University's Record Retention).

1. Notification

Authorized Users must report any incident of possible misuse of Institutional Data in the Cloud Commuting environment or violation of this Policy to the Information Technology Office.

2. Enforcement

IT is responsible for the appropriate enforcement of this Section. During any investigation of alleged inappropriate or unauthorized use of Institutional Data in the cloud computing environment, it may be necessary to temporarily suspend a un Authorized User's network or

computing privileges, but only after determining there is at least a prima facie case against the individual, as well as a risk to Technology Resources if privileges are not revoked. This is a necessary action taken to prevent further misuse and does not presume that the account holder initiated the misuse. Unsubstantiated reports will not result in the suspension of an Authorized User's account or network access unless sufficient evidence is provided to show that inappropriate activity occurred.

3. Sanctions

Employees and students who violate the provisions of the Section are subject to disciplinary action pursuant to the University's applicable disciplinary policies, as well loss of access to the University's Information Technology Resources.

Visitors and others third party users who violate the provisions of the policy are subject to loss of access to the University's Information Technology Resources. In addition, the Vice President for Finance and Treasurer may administer other appropriate sanctions.

BB. WIRELESS ACCESS POINTS

This section applies to all Authorized Users of University Wireless Access Points.

The purpose of this section is to establish University's procedures regarding the installation and use of Wireless Access Point on the University's campus.

In order to provide wireless access to authorized users IT installs "access points" in and around the campus. These access points are generally small, antenna-equipped boxes that connect directly to the local area network (LAN), converting the LAN's digital signals into radio signals. The radio signals are sent to the network interface card (NIC) of the Mobile Device (e.g. smartphone, IPad, laptop, etc.), which then converts the radio signal back to a digital format the Mobile Device can use. All users employing wireless methods of accessing the University's network must use University approved access points.

Personally-owned and unauthorized wireless access points that are installed without the knowledge or permission of IT and used by individuals to gain unauthorized access to the University's network are strictly prohibited. Any unapproved personal access point discovered in operation and connected to the University's network is subject to being disabled and/or removed immediately and indefinitely.

Use of the University wireless network is subject to the University's Acceptable Use Policy.

1. Wireless Access Point Approval

All wireless access points within the University's firewall must be approved and centrally managed by IT. The addition of new wireless access points within campus facilities will be managed at the sole discretion of IT staff.

IT will periodically conduct sweeps of the wireless network to ensure there are no unauthorized access points present.

IT reserves the right to turn off without notice any access point connected to the network that it feels puts the University's network or Institutional Data at risk.

Access point broadcast frequencies and channels are set and maintained by IT. Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, etc.

Wireless access users agree to immediately report to IT any incident or suspected incidents of unauthorized access point installation.

2. Enforcement

IT is responsible for the appropriate enforcement of this Section. During the course of any investigation of alleged inappropriate or unauthorized use, it may be necessary to temporarily suspend a user's network or Information Technology privileges, but only after determining there is at least a prima facie case against the individual, as well as a risk to the University network if privileges are not revoked. This is a necessary action taken to prevent further misuse and does not presume that an Authorized User initiated the misuse. Unsubstantiated reports will not result in the suspension of user account or network access unless sufficient evidence is provided to show that inappropriate activity occurred.

3. Disclaimer and Limitation of Liability

University makes no representations as to the performance, accuracy, or reliability of the University's Information Technology Resources. The University disclaims all warranties of any kind, expressed or implied, to the fullest extent permissible pursuant to applicable law, including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

By using the University's wireless access network, users agree that University, its trustees, or employees have no liability whatsoever for damages in any form under any theory of liability or indemnity in connection with an Authorized User's use of the University's Information Technology Resources, even if the University has been advised of the possibility of such damages. Users further recognize that the University has no control over the content of information servers on external electronic systems or the Internet accessed via the University's wireless network. The University, therefore, disclaims any responsibility and/or warranties for information and materials residing on non-University information servers on external electronic systems or the Internet. Such materials do not necessarily reflect the attitudes, opinions, or values of University.

CC. PEER-TO-PEER FILE SHARING

This Peer-to-Peer File Sharing section applies to all Authorized Users of the Technology Resources at University.

The purpose of this section is to provide for annual disclosures to students regarding the University's policies and sanctions related to unauthorized peer-to-peer file sharing, as required by the Higher Education Opportunity Act of 2008 (HEOA).

In compliance with the HEOA, it is the policy of the University to prohibit the use of peer-to-peer file sharing programs and applications for the unauthorized acquisition or distribution of copyrighted or licensed material on any University computer or University network. In addition, peer-to-peer file sharing programs and applications commonly used for these illicit purposes may not be installed on any applicable information technology resources, including a University computer, and technological deterrents will be used to block their use on the University network.

Authorized Users of the University's Technology Resources are prohibited from attempting attempt to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by the University to prevent the use of peer-to-peer file sharing programs and applications for the unauthorized acquisition or distribution of copyrighted or licensed material on any University computer or the University network. Legal alternatives to illegal file sharing practices include the use of services such as Apple iTunes, Netflix, Hulu, Amazon, Google Play Store, etc.

The University will annually inform students of this Section and associated procedures, consistent with the requirements of the HEOA.

1. Disclosure to Campus Community

The University will make readily available to the campus community, including enrolled and prospective students, the University's policies and sanctions related to peer-to-peer file sharing including: (i) a statement that explicitly informs individuals that unauthorized peer-to-peer file sharing may subject the student to civil and criminal liabilities; (ii) a summary of the penalties for violation of Federal copyright laws; and (iii) this Policy.

2. Notification of Violations

Authorized Users are requested to report any incident of possible misuse or violation of this Section to IT.

3. Enforcement

The CIO is responsible for the appropriate enforcement of this Section.

Alleged violations of the Digital Millennium Copyright Act (DMCA) are delivered to the CIO, who has been designated as the agent for the receipt of a claimed infringement. The CIO will respond to all DMCA notices. The receipts of such notices are to be logged in and tracked by the CIO. Attempts to identify the suspect computer(s) and user(s) will be made by IT staff upon direction of the CIO. In the case of suspected offenders who are students, if successful identification is made, a copy of the notice and name of student(s) identified will be referred to the Office of Student Affairs. In the case of suspected faculty or staff who are successfully identified, the notice and name of the staff or faculty member(s) and relevant identifying information will be referred to Human Resources or the Provost and Vice President for Academic Affairs as applicable. In circumstances when criminal activity is suspected, the CIO will consult with Campus Safety and Security before notifying any party.

During the course of any investigation of alleged unauthorized peer-to-peer file sharing, it may be necessary to temporarily suspend an Authorized User's network or computing privileges, but only after determining there is at least a prima facie case against the individual. This is a necessary action taken to prevent further misuse and does not presume that the account holder initiated the misuse. Unsubstantiated reports will not result in the suspension of user account or network access unless sufficient evidence is provided to show that inappropriate activity occurred.

4. Sanctions

Students and employees who violate the provisions of the Section are subject to disciplinary action pursuant to the University's applicable disciplinary policies, as well loss of access to the university's Technology Resources.

Visitors and others third party users who violate the provisions of the Section are subject to loss of access to the University's information technology resources. Moreover, the Vice President for Finance and Treasurer may administer other appropriate sanctions.

In addition to the above, violators of this Section may be subject to criminal and civil sanctions. A summary of the current civil and criminal penalties for violation of federal copyright laws is as follows:

- The infringer may be required to pay the actual dollar amount of damages in an amount equal to the profits gained from the infringement or, alternatively, pay what are termed "statutory damages." Statutory damages can range from $750 to $30,000 for each work infringed, unless the court finds that the infringement was willful. In such cases, the maximum penalty is increased to $150,000.
- The court may also award attorney fees and court costs, issue an injunction to stop the infringing acts and impound the illegal works.
- The infringer can be sent to jail for up to 10 years.

DD. ELECTRONIC PRIVACY STATEMENT

This Website Privacy section applies to all information collected by or submitted to official websites of University and to all visitors to these websites.

The purpose of this section is to ensure that all official University websites include an electronic privacy statement about the information that is collected by their website (both automatically and voluntarily) and how that information is used.

All official University websites will be required to adhere to the privacy and practices the University has adopted for its official websites as outlined in this Policy and inform visitors of how information at that site is managed through the posting of an electronic privacy notice. Individual websites may either link to this Policy or develop specific notices about the collection and use of any information associated with their pages consistent with the University's policies.

1. Privacy Notice

The following information outlines the electronic privacy policy and practices University has adopted for its official websites. The policy and corresponding practices shall not be construed as a contractual promise and the University reserves the right to amend this Section at any time without notice.

a. Collection and Use of Information: When visiting a University website, the University permits the following information to be collected and stored:

a. Access Information (Automatically Collected):

i. Client Information: Routing information such as the Internet domain and Internet address of the computer being used.

ii. Essential Technical Information: identification of the page or service being requested by the user, the type of browser and operating system being used and the date and time of access.

b. **Personal Information Voluntarily Provided by the Individual (Optional Information):** When visiting a University website (e.g. sending an email message, filling in an on-line form, etc.), individuals may choose to provide additional Personally Identifiable Information such as name, address, email address, social security number, password, bank account information, credit card information, or any combination of data that can be used to identify an individual.

2. **Use of Information:** University does not track individual visitor profiles. It does, however, analyze aggregate traffic/access information for resource management and site planning purposes. The University reserves the right to use log detail to investigate resource management or security concerns.

a. Access Information

i. Client Information is used to route the requested webpage to the user's computer for viewing. The requested webpage and the routing information could be discerned by other entities involved in transmitting the requested page to the user. The University does not control the privacy practices of those entities.

ii. The University may keep client information from its systems indefinitely after the Webpage is transmitted, but it does not cross-reference it to the individuals who browse the University's Website. However, on rare occasions when a "hacker" attempts to breach computer security, logs of access information are retained to permit a security investigation. In such cases, the logs may be further analyzed or forwarded together with any other relevant information in the University's possession to law enforcement agencies.

iii. Essential and nonessential technical information let the University respond to the user's request in an appropriate format and helps the University plan Website improvements. To expedite this process, some official University Websites use "cookies." Cookies are small pieces of data passed from a website to the user's hard drive to enable some online services to work more efficiently or to make the use of services more convenient. The University generally will not use cookies to track and/or retain Personally Identifiable Information without proper notification. However, the University reserves the right to associate Personally Identifiable Information with cookies. Such information will not be disclosed to outside parties unless legally required to do so in connection with legal proceedings or law enforcement investigations.

iv. The University also uses non-identifying and aggregate information to better design its Website. The University, however, does not disclose information that could identify specific individuals.

b. Optional Information:

i. Optional Information enables the University to provide services or information tailored more specifically to the individual user's needs, to

forward a user message or inquiry to another entity that is better able to do so, and to plan Website improvements.

ii. The University uses the information to provide only to complete that order or request. It generally does not share this information with outside parties, except to the extent necessary to complete that order or request. In those cases, the University will ensure that the third party has formally agreed to protect the security of that data in compliance with the University's Information Security Plan.

iii. The University generally uses return e-mail addresses only to answer the e-mail it receives. Such addresses are generally not used for any other purpose and are not shared with outside parties. It should be understood, however, that it is impossible to assure the privacy of email. Not only may email be sent to someone other than the intended recipient (either through mis-addressing or forwarding), but email sent as plain text may also be intercepted as it travels over the network. In addition, as part of the University's backup and archival practices, email may continue to exist.

iv. The University never uses or share the Personally Identifiable Information provided to it online in ways unrelated to the purpose described without a clear notice on the particular site and without also providing the individual an opportunity to opt-out or otherwise prohibit such unrelated uses.

3. **Links:** The provision of links from official University websites to other sites does not imply endorsement of the information or services offered by these linked sites nor does the University's privacy policies apply to these other sites. Individuals who choose to link to any third party site should review the privacy practices of that site before providing any Personally Identifiable Information to that site.

4. **Children Policy**: Children under the age of 13 are not allowed to register on University websites, or to access areas that require registration. If the University learns that it has inadvertently collected information from an individual under the age of 13, that information will be immediately and permanently removed from the University's servers.

EE. RECORD RETENTION (See next page)

General Record Retention Schedule

Type of Record	Retention Period	Official Repository	Paper Copy	Electronic Copy	Authority
GOVERNANCE & CORPORATE RECORDS					
Articles of Incorporation, Amendments, Bylaws	Permanent	President's Office	yes		Legal Counsel
Annual Reports	30 Years	Archives	yes	yes	Legal Counsel
Organizational Charts	10 years	President	yes	yes	Legal Counsel
Board of Trustees Meeting Minutes	Permanent	President & Archives			
Accreditation documents-Self Study and Accreditation Letters	Self study reports are retained until the next review; Visiting team documents and report and the accreditation are retained permanently.	President & Archives	yes		Historical Relevance
Awards issued by the Board Record of candidates	Permanent – part of Board minutes	President & Archives	yes		Historical Relevance
Board of Trustee Member Records	Permanent	President & Archives	yes		Historical Relevance
Institutional Strategic Planning Records	Permanent for final planning reports 10 years for internal planning committee		yes	yes	Historical Relevance
Mission Statements	Permanent	President	yes	yes	Historical Relevance
Committee Records	Permanent	President Archives	yes		Historical Relevance
STUDENT ACADEMIC RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Admissions – Enrolled Students					

Type of Record	Retention Period	Official Repository	Paper Copy	Electronic Copy	Authority
Admissions Letter	5 Years After Separation		yes		American Association of Collegiate Registrars and Admissions Officers (AACRAO) Guideline
Correspondence	5 Years After Separation		yes		AACRAO
Application Materials – Enrolled Students	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Advanced Placement, CLEP, and PEP Records	5 Years After Separation		yes		AACRAO
Applications for Admissions or Re-admissions	5 Years After Separation		yes		AACRAO
Entrance Exam Reports	5 Years After Separation		yes		AACRAO
Health, Immunization and Other Documentation Records	5 Years After Separation		yes		AACRAO
Supporting Documentations (e.g., Letters of Recommendation, Resumes and Essays)	Until Admitted		yes		AACRAO
High School and Other College Transcripts	5 Years After Separation		yes		AACRAO
Military records	5 Years After Separation		yes		AACRAO
Release from High School or Dual Enrollment forms	3 Years After Separation		yes		AACRAO
Residency Classification forms	5 Years After Separation		yes		AACRAO
Test scores (other)	5 Years After Separation		yes		AACRAO
International Student Documents (enrolled)	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Alien registration receipt card	5 Years After Separation		yes		AACRAO
DS-2019	5 Years After Separation		yes		AACRAO

Type of Record	Retention Period	Official Repository	Paper Copy	Electronic Copy	Authority
Employment authorization	5 Years After Separation		yes		AACRAO
I-20	5 Years After Separation		yes		AACRAO
I-94	5 Years After Separation		yes		AACRAO
Passport Number	5 Years After Separation		yes		AACRAO
Statement of educational costs	5 Years After Separation		yes		AACRAO
Statement of financial responsibility	5 Years After Separation		yes		AACRAO
Admissions Records– Non-Enrolled Students	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Admissions Letters	1 year after application		yes		AACRAO
Correspondence	1 year after application		yes		AACRAO
Application for admission or re-admission	1 year after application		yes		AACRAO
Credit by Examination	5 years after graduation or non-attendance		yes		AACRAO
Entrance Examinations/text scores	1 year after application		yes		AACRAO
Medical Records	1 year after application		yes		AACRAO
Letters of recommendation (Admissions)	1 year after application		yes		AACRAO
Military Records	1 year after application		yes		AACRAO
Placement text records/scores	1 year after application		yes		AACRAO
Residency classification forms	1 year after application		yes		AACRAO
Test scores (other)	1 year after application		yes		AACRAO
Transcripts	1 year after application		yes		AACRAO
International Student Documents (non-enrolled)	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Alien registration receipt card	1 year after application		yes		AACRAO
DS-2019	1 year after application		yes		AACRAO

Type of Record	Retention Period	Official Repository	Paper Copy	Electronic Copy	Authority
Employment authorization	1 year after application		yes		AACRAO
I-20	1 year after application		yes		AACRAO
I-94	1 year after application		yes		AACRAO
Passport Number	1 year after application		yes		AACRAO
Statement of educational costs	1 year after application		yes		AACRAO
Statement of financial responsibility	1 year after application		yes		AACRAO
Curriculum, Instruction, Enrollment Report Records	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Course Enrollment Summaries; Graduation Summaries; Registration Reports; etc.	Permanent				Historical Relevance
Course Catalog and Schedule of Courses	Permanent (1 Copy)				Historical Relevance
Course Proposals	Permanent				Historical Relevance
Degree Requirements	Permanent				Historical Relevance
Student Surveys (Instrument and Results)	7 Years				
New Degree Records	Permanent				Historical Relevance
Program Development and Review Records	Permanent				Historical Relevance
Syllabi	1 Academic Year				
Degree, Grade, Enrollment, and Racial/Ethnic Statistics	Permanent				Historical Relevance
FINANCIAL AID RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Borrowers Loan Records (Institutional and Perkins Loans, Repayment Schedules, Statement of Rights and Responsibilities, Records of Actions Taken, Related Correspondence)	3 Years after the loan is paid in full or assignment to the Department of Education		yes – student file		34 C.F.R. § 668.24

Type of Record	Retention Period	Official Repository	Paper Copy	Electronic Copy	Authority
Federal Title IV, Program Records, Institutional Records • Accreditation Reviews and Reports • Any other record pertaining to factors of financial responsibility and standards of administrative capability • Audits and Program Reviews • Education Program Eligibility • Institutional Program Participation Agreement • Recertification	Agreements: 6 years after expiration 3 years after the end of the award year in which the report was submitted; Records pertaining to audit and program reviews must be retained until resolution of the matter is reached.		yes – student file		34 CFR 668.24
Federal Family Education Loan and Direct Program Records • Applications • Disbursement Records • Promissory Notes • Student Status Confirmation Reports	3 years after the end of the award year in which the student borrower last attended the University		no		34 C.F.R. § 668.24
Financial Aid Annual Reports	3 years after the end of the award year		yes – student file		34 C.F.R. § 674.8(c)

Type of Record	Retention Period	Official Repository	Paper Copy	Electronic Copy	Authority
Fiscal Records and Reports • Accreditation and Licensing Agency Reports • Annual Federal Fiscal Operations and Applications for Funds Report • Cash Disbursements • Federal Pell Grant Statements of Account • Federal Work-Study Payroll Records • General Ledgers • Refunds and Repayments • State Grant and Scholarship Award • Financial Aid Office Rosters and Reports • Title IV Program Reconciliation Reports	3 years after the end of the award year for which the report was submitted		yes – student file		34 C.F.R. § 674.8(c)
Pell Grant Reports	3 years after the end of the award year for which the award was submitted		no		34 CFR § 668.24
Perkins Promissory Notes and Repayment Schedules	Until loan is satisfied		yes – student file		34 CFR § 668.24
Perkins Loan Repayment Records	3 years from date loan assigned, cancelled, or repaid		yes – student file		34 CFR § 668.24
Work Study Program Administrative Records	3 years After Separation		yes – student file		34 CFR § 668.24
STUDENT ACADEMIC RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Academic Advising Records	5 Years After Separation				AACRAO
Name Change Authorization	10 Years After Separation				AACRAO
Audit Authorizations					AACRAO

Type of Record	Retention Period	Official Repository	Paper Copy	Electronic Copy	Authority
Student Academic Warning, Probation Records	5 Years After Separation				AACRAO
Academic Dismissal	Permanent				AACRAO
Academic Integrity Violations	Permanent				
Change of Major/Minor, Certification of 2nd Major/Minors	5 years after graduation				
Student Requests for Nondisclosure of Directory Information and Consents to Disclose Identifiable Information	Until terminated by the student or permanent				AACRAO
Changes of Course (Add/Drop)					AACRAO
Audit Authorizations					AACRAO
Class Rosters/Lists	Permanent				Historical Relevance
Student Commencement Records	Permanent				Historical Relevance
Student Course Offerings	Permanent				Historical Relevance
Student Curriculum Change Authorizations	5 Years After Graduation				AACRAO
Student Examinations, Tests, Term Papers, Homework	5 Years After Graduation		yes		AACRAO
Student Grade Reports to Registrar	1 Year After Date Submitted				AACRAO
Student Graduation Authorization	5 Years After Graduation		yes		AACRAO
Student Hold	Until Released		yes		AACRAO
Student Internship Program Records	5 Years After Graduation		yes		AACRAO
Student Class Schedules	1 Year After Separation		yes		AACRAO
Student Thesis and Dissertation Records	Permanent		yes		AACRAO
Student Transcripts	Permanent		yes		AACRAO
Student Transfer Credit Evaluations	5 Years After Separation		yes		AACRAO
Student Withdrawal Authorizations	5 Years After Graduation		yes		AACRAO
Leaves of Absence	2 years				AACRAO

Type of Record	Retention Period	Official Repository	Paper Copy	Electronic Copy	Authority
Study Abroad Records	5 years After Separation				
Study Abroad Student Records	5 years After Separation		yes		AACRAO
Certification/ Verification Records					
Enrollment Verification	1 year after certification				
Residency Verification records	6 years after submission				
Teacher certifications	1 year after certification				
Student Transcript Requests	1 Year After Requested		yes		AACRAO
BUSINESS, FINANCE & ACCOUNTING RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Accounts Payable Ledgers & Schedules	7 years				IRS/Better Business Bureau
Accounts Receivable Ledgers & Schedules	7 years				IRS/Better Business Bureau
Audit Reports	Permanent				IRS/Better Business Bureau
Bank Reconciliations	2 years				IRS/Better Business Bureau
Bank Statements	3 years				IRS/Better Business Bureau
Capital Stock & Bond Records: ledgers, transfer registers, stubs showing issues, record of interest coupons, options, etc.	Permanent				IRS/Better Business Bureau
Cash Books	Permanent				IRS/Better Business Bureau
Charts of Accounts	Permanent				IRS/Better Business Bureau
Checks (cancelled –see exception below)	7 years				IRS/Better Business Bureau
Checks (cancelled for important payments – i.e., taxes, purchases of property, special contracts, etc. Checks should be filed with the	Permanent				IRS/Better Business Bureau

papers pertaining to the underlying transaction.)					
Contracts, mortgages, notes, and leases (expired)	7 years				IRS/Better Business Bureau
Contracts, mortgages, notes & leases (still in effect)	Permanent				IRS/Better Business Bureau
Correspondence (general)	2 years				IRS/Better Business Bureau
Correspondence (legal & important matters)	Permanent				IRS/Better Business Bureau
Correspondence (routine) with customers and/or vendors	2 years				IRS/Better Business Bureau
Deeds, mortgages & bills of sale	Permanent				IRS/Better Business Bureau
Depreciation schedules	Permanent				IRS/Better Business Bureau
Duplicate deposit slips	2 years				IRS/Better Business Bureau
Expenses analyses/expense distribution schedules	7 years				IRS/Better Business Bureau
Financial Statements (year-end, other optional)	Permanent				IRS/Better Business Bureau
General/private ledgers, year-end trial balance	Permanent				IRS/Better Business Bureau
Insurance policies (expired)	3 years				IRS/Better Business Bureau
Insurance records, current accident reports, claims, policies, etc.	Permanent				IRS/Better Business Bureau
Internal Audit reports (longer retention periods may be desirable)	3 years				IRS/Better Business Bureau
Internal Reports (miscellaneous)	3 years				IRS/Better Business Bureau
Invoices (to customers, from vendors)	7 years				IRS/Better Business Bureau
Journals	Permanently				IRS/Better

					Business Bureau
Notes receivable ledgers & schedules	7 years				IRS/Better Business Bureau
Option records (expired)	7 years				IRS/Better Business Bureau
Patents & related papers	Permanent				IRS/Better Business Bureau
Petty Cash vouchers	3 years				IRS/Better Business Bureau
Physical inventory tags	3 years				IRS/Better Business Bureau
Plant cost ledgers	7 years				IRS/Better Business Bureau
Property appraisals by outside appraisers	Permanent				IRS/Better Business Bureau
Property records, including costs, depreciation reserves, year-end balances, depreciation schedules, blueprints, and plans	Permanent				IRS/Better Business Bureau
Purchase orders	7 years				IRS/Better Business Bureau
Receiving sheets	1 year				IRS/Better Business Bureau
Requisitions	1 year				IRS/Better Business Bureau
Sales records	7 years				IRS/Better Business Bureau
Scrap and salvage records (inventories, sales, etc.)	7 years				IRS/Better Business Bureau
Stocks and Bonds certificates (cancelled)	7 years				IRS/Better Business Bureau
Subsidiary ledgers	7 years				IRS/Better Business Bureau
Tax Returns & worksheets, revenue agents' reports, and other documents relation to determination of income tax liability	Permanent				IRS/Better Business Bureau

Trademark registrations/copyrights and patents	Permanent				IRS/Better Business Bureau
Training Manuals	Permanent				IRS/Better Business Bureau
Voucher registers & schedules	7 years				IRS/Better Business Bureau
Vouchers for payment to venders, employees, etc. (including allowances and reimbursement of employees for travel and entertainment expenses)	7 years				IRS/Better Business Bureau
RESEARCH & SPONSORED PROGRAMS RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Administrative and Financial Records					
Grants, contracts, and cooperative agreements including funded proposals	Three (3) years from date of submission of the final report unless a longer retention period is specified under the agreement or grant rules		yes		20 USC § 1232f(a); 34 C.F.R. § 74.53; 2 CFR 215.53; OMB Circular A-110 - subpart C-53 Historical Relevance
All financial records, documentation and reports pertinent to an award (Federal, State, Private)	Three (3) years from date of submission of the final report unless a longer retention period is specified under the agreement or grant rules.		yes		2 CFR 215.53; OMB Circular A-110 - subpart C-53 Historical Relevance
Supporting documents and statistical records pertinent to a federal, state or private award	Three (3) years from date of submission of the final report unless a longer retention period is specified under the agreement or grant rules.		yes		20 USC § 1232f(a); 34 C.F.R. § 74.53; 2 CFR 215.53; OMB Circular A-110 - subpart C-53 Historical Relevance

Basic Research Records	Retention Period	Official Repository	Paper Copy	Electronic Copy	Authority
Research Data	Three (3) years after submission of the final report of the research to the sponsor, unless a longer retention period is specified under the agreement or grant rules.* * If pediatric research, until the youngest subject turns twenty-five years old.				2 CFR 215.36 /Intangible Property OMB Circular a-110 Subpart C-36
Conflict of Interest forms (NSF and PHS funded studies)	3 years or as determined by individual award agreement				NSF Grant Policy Manual Chapter V Section 510; 42 CFR 50.604
Research misconduct records	7 years after completion of the proceeding or the completion of any PHS proceeding involving the research misconduct allegation under subparts D and E of 42 CFR 93.317, whichever is later.				42 CFR 93.317
Human Subject Research	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Human Subject Research related records including research results, research and regulatory records, research proposals, publication, consent forms, etc.).	Five years after the completion of the research, either electronically or as hard copy. In accordance with federal HIPAA privacy regulations,				45 CFR 46.115(b) and 21 CFR 56.115(b); 45 CFR § 164.530(j)

	records containing protected health information (PHI) are retained for at least six years after the completion of the research.				
Research Ethics and Review Board Records, including membership lists, training materials, review and approval records, policies and procedures, investigations of non-compliance, etc.).	5 years after the completion of the research				45 CFR 46.115(b) and 21 CFR 56.115(b)
UNIVERSITY ADVANCEMENT, COMMUNICATIONS & GOVERNMENT RELATIONS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
University Advancement Records					
Gift Receipts	Seven years		yes		26 USC § 6501
Fund Raising Records	Current year plus seven years				
Endowment - Donor Records and Agreements	Permanent as determined by needs of University		yes		Historical Relevance
Planned Giving Documents	Permanent as determined by needs of University		yes		Historical Relevance
Donor Agreements Related to all other Gifts/Donations	Permanent as determined by needs of University		yes		Historical Relevance
University Advancement Planning Records	Permanent as determined by needs of University		yes		Historical Relevance
Monthly Gifts and Grant	3 years after the submission of the				

Reports	final financial report				
Giving Reports	7 years after report is created				
Donor & Development Records (Records that document the efforts to establish relationships with alumni, the community groups, individuals, and businesses, to gain their assistance with the development and coordination of institutional programs. File may include reports, brochures, newsletters or publications, agendas, minutes, correspondence, and other related records)	Retain agendas, minutes, publications, newsletters, brochures permanently. Retain all other records for current year plus seven years				
Alumni Records	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Alumni Membership Lists, Mailing List and Related Correspondence	Permanent		yes		Historical Relevance
University Communication Records	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Photographs, video, other Images (Including Supporting Photography Consent Form, Release, Waiver, or Similar Necessary Authorizations)	Permanent as Determined by Historical Relevance – One Copy		yes		Historical Relevance
Advertising and Public Relations Materials	Permanent as Determined by Historical Relevance (One Copy) or One year as determined by University		yes		Historical Relevance; 38 USC § 3696
University Publications (Including Source Records Supporting	Permanent as Determined by Historical		yes		Historical Relevance

Publications)	Relevance – One Copy				
University Wide Events Event Records (e.g. Guest List, Invitations, Seating Charts, Brochures, Agenda and Other Materials Memorializing the Event)	Permanent as Determined by Historical Relevance – One Copy		yes		Historical Relevance
Government Relation Records	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Government & Community Relations Records (e.g. Federal, State and Local Lobbying & Legislative Records, Reports and Correspondence with Government Agencies)	Permanent		yes		Historical Relevance
STUDENT LIFE RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Student ADA Records					
ADA Student Accommodation Records File (e.g. Request for Accommodation, Supporting Documents, Letter of Accommodation, Signed Released Forms, Correspondence)	5 Years from close of academic term		yes		29 C.F.R. Section 1602.14
ADA Accommodation Records for Testing	5 Years from close of academic term		yes		29 C.F.R. Section 1602.14
Athletic Records	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Records maintained according to NCAA Bylaws**
Eligibility Records	6 Years				
Game Statistics	Permanent		yes		Historical Relevance

Individual Student-Athletes Records: Academics Eligibility Equipment Insurance Physical	6 Years after separation		yes		
Compliance Records	6 Years		yes		
Press Clippings	Permanent		yes		Historical Relevance
Recruiting Records	6 Years		yes		
Photographs (Student-Athletes, Coaches, Staff)	Permanent		yes		Historical Relevance
Student Athlete Academic Advising Records	7 Years		yes		
Student Athlete Medical Records	7 Years		yes		
Non-Academic Student Records	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Student Judicial and Student Conduct Records (Findings of Violation and Related Case Files)	5years after graduation or separation		yes		AACRAO
Student Grievances (not grade appeals)	3 years after closure				AACRAO
Student Organizations Event Records	5 Years		yes		
Student Organization Recognition Paperwork	7 Years		yes		
Student Tuition and Fee Charges	5 Years After Separation		yes		AACRAO Guideline
HUMAN RESOURCE RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Job Announcements and Advertisements	2 years				29 CFR § 1627.3(b); Legal Counsel
Individual Applicants Who Are Not Hired	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Employment Applications, Resumes	3 years after search completed		yes		29 CFR 1602.14 29 CFR 1602.21;

					Legal Counsel
Background Investigation Results	3 years after search completed		yes		29 CFR 1602.14 29 CFR 1602.21
Resumes	3 years after search completed		yes		29 CFR 1602.14 29 CFR 1602.21
Letters of Recommendation	3 years after search completed		yes		29 CFR 1602.14; 29 CFR 1602.21
Employees	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Employee Personnel Files	7 years following separation		yes		29 USC 1027; Legal Counsel
Employee Benefit Files	7 years after discontinuation or change of benefits		yes		29 USC 1027; Legal Counsel
403(b) Application) Records and Retirement Plan Documents	Permanent		yes or		Legal Counsel
Required Personal Information Employees (Name, Address, SS#, Pay, Hourly or Salaried)	7 years after separation				Legal Counsel
Payroll records & summaries	7 years				
ADA Records	5 years after separation		yes		29 C.F.R. Section 1602.14
Continuation of Insurance Benefits (COBRA) Records	4 years		yes		Legal Counsel
Family and Medical Leave Case Files	3 years after employee separation		yes		29 C.F.R. §825.500.
I-9 Forms and other Employment Verification Records	3 years after hire or 1 year after separation, whichever comes later		yes		8 U.S.C. §1324; 8 C.F.R. § 274a.2
Job Descriptions	3 years		yes		29 CFR § 516.6; 29 CFR § 1620.32
Promotion and Salary Increase Records	7 years after separation		yes		29 USC 1027
Unemployment Compensation Claims,	7 years		yes		Legal Counsel

Unclaimed Salaries					
Workers' Compensation Claims	10 years		yes		Legal Counsel
Faculty meeting minutes	Permanent		yes		Historical Relevance
Faculty promotion, tenure records, and tenure-review records	7 years after separation		yes		29 USC 1027
Student Evaluations of Faculty Courses	3years after completion of course		yes		Legal Counsel
Payroll Records – Individual Employees	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Payroll Additions/Deductions Overtime Authorization	4 years				FICA; 29 U.S.C. Sections 201-219; 28 U.S.C. Section 1658; 29 CFR 516.5; 29 CFR 516.6
Time Cards or Sheets	7 years				29 U.S.C. Sections 201-219; 28 U.S.C. Section 1658; 29 CFR 1627.3
Employment Tax Related Records (W-2, W-4, 1099, returns, schedules, etc.)	Until superseded or 7 years after separation				26 C.F.R. Sections 31.6001-1 to 31.6001-6;
Garnishments	7 years				IRS and Better Business Bureau
INFORMATION TECHNOLOGY RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Computer Performance Reports, Security Documentation	5 years	IT			Legal Counsel
System Documentation, Systems Maintenance Documents, Source Code Listings and Updates	5 years	IT			Legal Counsel
Computer Performance Reports, Security Documentation	5 years	IT			Legal Counsel
Vendor Service Orders, Tape Backup Records	5 years	IT			Legal Counsel

Website Records (records that document the development of a web site for a unit. File may include drafts of content, specifications, software product, and other related information)	Retain until administrative usefulness is completed then dispose of.	IT			
ENVIRONMENTAL HEALTH & SAFETY RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Environmental Regulations Records (Documentation of institutional compliance with environmental laws and guidelines of federal, state, or local governments.)	10 years				
Training Records (OSHA)	30 years from the date on which training occurred after employee separates				29 CFR 1910.1020
Toxic Substance Exposure Records	30 years				29 CFR 1910.1020
Fire Safety Records, Audit Reports	Permanent				Legal Counsel
Drug Screening, Employee Asbestos Monitoring, Employee Exposure Records, Employee Medical Records, Employee Medical and Exposure Records	30 years after separation				OSHA 1910.1001; OSHA 1910.20; OSHA 1910.1025
Accident Reports (OSHA)	30 years after termination				Legal Counsel
Chemical and Hazardous Waste Disposal Records	30 years				40 CFR 262.20
Material Safety Data Sheets Records	30 years from the date the substance was last received in the workplace				29 CFR 1910.1020
LEGAL RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**

Contracts, Closing Documents, Due Diligence Files	Permanent				Legal Counsel
Patent Files, Research Files, Trademark Registrations, Copyright Registrations	Permanent				Legal Counsel
Regulatory Filings, Government Investigation Files	Permanent				Legal Counsel
Other Litigation and Investigations	Permanent				Legal Counsel
SECURITY RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Dispatch Records	3 years, or until case is adjudicated, whichever is longer				
Clery Act Crime and Fire Report and all supporting records (copies of crime reports; the daily crime logs; records for arrests and referrals for disciplinary action; timely warning and emergency notification reports; documentation, such as letters to and from local police having to do with Clery Act compliance; letters to and from campus security authorities; correspondence with us regarding Clery Act compliance; and copies of notices to students and employees about the availability of the annual security report)	3 years from the latest publication of the report to which they apply (in effect 7 years)	Public Safety	yes	yes	20 USC § 1092
Property Damage Reports	4 years after report date or three years until case is				

	closed.				
Vehicle Accident	7 years				
DMV Lists	Until superseded				
Key Issuance	2 years after key is returned				
Parking Citations	2 years after resolution				
Parking Permits	2 years				
Bicycle License/Registration	2 years				
LIBRARY	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Requests for items to be put on reserves	Current semester	LIB			
Security incident reports	Permanent	LIB			
ILL records of request	current semester	LIB			
Circulation for journals (not including patron record)	1 year	LIB			
Materials checked out (by patron)	Until returned	LIB			
Fine records	Until paid	LIB			
Circulation system user records	While user is active	LIB			
Initial order records for books, serials, and e-resources	Permanent	LIB			
Accounting reports/deposit receipts from service desks	10 years	LIB			
Library budget	10 years	LIB			
Library statistics	Permanent	LIB			
Library publications (e.g., manuals, handbooks, etc.)	While active; then transfer to Archives	LIB			
Graduate Theses and Dissertations	Permanent	LIB			
Appraisal of Library Materials	Permanent	LIB			

Artifact Acquisition/Special Collection Records	Permanent	LIB			
Collection & Acquisition Exchange	While active	LIB			
Serial Records	While active	LIB			
TITLE IX RECORDS	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Title IX Audit Records	3 Years	Title IX Coordinator	Yes	Yes	Per Title IX, An educational institution must evaluate its current policies and procedures as they affect the admission of students, treatment of students, and employment of both academic and non-academic personnel working in connection with the provider's education program or activity. See Title IX Legal Manual, pp. 108-109
Title IX Reporting, Investigation and Resolution Records: This series documents the investigation and outcome of alleged violations of the sexual misconduct policy. This series may include, but is not limited to: incident reports, notification of	7 years from final resolution				

allegation, hearing notes, decision statements, appeals documentation, and final report.					
FACILITIES MANAGEMENT	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Vehicle Inspection	4 years				
Vehicle Records	4 years after disposal of vehicle				
Utilities System Operating & Maintenance	3 years after equipment is no longer in service				
Work Order Requests	4 years				
Permit drawings, record drawings	Permanent/Life of facility				
Building /Land Inventory	Permanent				
Certificates of Occupancy	Permanent/Life of facility				
Building Permits	Permanent/Life of facility				
Space/Facilities Use	5 years for summary reports/Permanent for overall historical information/ Archives receives perm. documents				
Plats, surveys, utility location maps	Permanent/Life of facility				
INSTITUTIONAL RESEARCH	**Retention Period**	**Official Repository**	**Paper Copy**	**Electronic Copy**	**Authority**
Grade Distribution Reports	Permanent	Institutional Research			

Statistical Abstracts	Permanent	Institutional Research			
Statistical Year in Reviews	Permanent	Institutional Research			
Various Ad Hoc Reports	5 years	Institutional Research			
IPEDS Reports	Permanent	Institutional Research			
State Ed Reports	Permanent	Institutional Research			
NCAA Reports	Permanent	Athletics			
Commercial Surveys (US News, etc.)	5 years	Institutional Research			
Faculty Data	Permanent	Institutional Research			
Student Data	Permanent	Institutional Research			
Course Data	Permanent	Institutional Research			
Survey Data	Permanent	Institutional Research			
NSF Data	Permanent	Institutional Research			
Department Reviews	Permanent	Institutional Research			

FF. LEGAL HOLD RELEASE (See next page)

Appendix: Legal Hold Form

Attorney-Client Privileged Communication

Confidential Attorney Work Product

TO:

FROM:

DATE:

RE: IMPORTANT DOCUMENT RETENTION ALERT

Summary of Lawsuit:

The University has recently brought an action against (or has been named as a defendant by) _____

The Complaint alleges _____

In connection with the lawsuit,_____is entitled to review and inspect documents relating to the allegations in the Complaint. Consequently, please follow this important instruction:

UNTIL FURTHER NOTICE FROM AU'S LEGAL COUNSEL, YOU ARE TO PRESERVE AND ARE NOT TO DELETE, DISCARD, OR OTHERIWSE DESTROY ORIGINAL AND ALL COPIES OF ALL DOCUMENTS, WHETER IN ELECTRONIC FORM OR HARD COPY, INCLUDING WITHOUT LIMITATION, CORRESPONDENCE (INCLUDING EMAIL), MEMORANDA, FAXES, CHARTS, LANS, GRAPHS, TELEPHONE SLIPS AND NOTES, PHOTOGRAPHS, DATABASES, BACK UP TAPES AND ANY AND ALL OTHER DOCUMENTS OR TANGIBLE MATERIALS WITH RESPECT TO THE AFOREMENTIONED COMPANY, PERSON(S), AND/OR SUBJECTS LISTED BELOW.

Categories of Relevant Documents:

For purposes of these categories, unless otherwise indicated in the bullet-points below, the relevant timeframe is from_____to the present. The categories include:

- Documents relating to_____.
- Documents evidencing any communication with_____.
- Documents regarding_____.
- Documents discussing_____.
- Documents reflecting communications with_____.
- Documents that evidence an agreement by or among_____, including_____to_____.
- Documents that analyze, discuss or consider_____.

Document Production and Chain of Custody Considerations:

As the litigation progresses, we will coordinate with you through Legal Counsel and/or Outside Counsel **xxxx**) to gather the above-referenced (electronic and hard copy) documents. At the relevant time, we will ask you to include in the scope of your search the following locations:

- Immediate work space (including cabinets, desk, filing cabinets, redwells, journals, work logs or diaries, calendars);
- Electronic hardware and software (desktop computer, laptop, hand held devices, including Palm Pilots, Treos, Blackberries, etc.);
- Home office, to the extent that you retain work-related documents at home.

Once you are asked and you begin gathering responsive documents, we also will ask you to make note of the exact location from which you will conduct your search for documents. We also will want you to provide information relating to responsive documents that you know are located at off-site storage or other locations.

Scope of Obligation:

If you believe you have other documents not covered by the above categories that somehow relate to these specific areas or to AU's investigation of the claims in general, please save them as well.

THIS ALERT SUPERSEDES ANY CONTRARY INSTRUCTIONS IN THE UNIVERSITY'S POLICIES AND PROCEDURES, AND ANY OTHER GUIDELINE YOU MAY HAVE RECEIVED CONCERNING THE RETENTION OF RECORDS, DOCUMENTS AND OTHER ITEMS.FAILURE TO FOLLOW IT STRICTLY CAN RESULT IN SERIOUS LEGAL AND OTHER CONSEQUENCES FOR YOU AS WELL AS THE UNIVERSITY.

You should share this memorandum with anyone in your department you believe has or might have documents related to the above categories specifically or to the University's investigation of the claims in general.

When you identify other members of your department who may have relevant data and forward this memo on to them, please copy Legal on the e-mail.

Procedures for Identification and Search:

As indicated, Legal Counsel and/or outside counsel retained to represent the university will be following up with you as the litigation progresses and as necessary to collect any and all responsive documents from you and members of your staff.

A subsequent memo containing instructions likely then will be distributed. In the meantime, please do not remove any responsive documents or materials from their present location.

If you have any questions about this alert or how to implement or interpret it, contact _____in the University's Legal Counsel. Thank you.

Appendix: Legal Hold Release Form

Attorney-Client Privileged Communication

Confidential Attorney Work Product

TO:

FROM:

DATE:

RE: LEGAL HOLD RELEASE

IN ACCORDANCE WITH THE UNIVERSITY'S RECORDS RETENTION POLICY, YOU ARE HEREBY NOTIFIED THAT THE LEGAL HOLD PERTAINING TO THE FOLLOWING SUBJECT MATTER IS RELEASED. PLEASE RETURN ALL RECORDS RELEVANT TO THE LEGAL HOLD TO THEIR NORMAL HANDLING PROCEDURES AND RETENTION SCHEDULES.

Categories of Relevant Documents:

For purposes of these categories, unless otherwise indicated in the bullet-points below, the relevant timeframe is from_____to the present. The categories include:

- Documents relating to_____.
- Documents evidencing any communication with_____.
- Documents regarding_____.
- Documents discussing_____.
- Documents reflecting communications with_____.
- Documents that evidence an agreement by or among_____, including_____to_____.
- Documents that analyze, discuss or consider_____.

IV. DEFINITIONS

Academic Technology Services Advisory Committee: Provides leadership for educational technology initiatives by fostering collaboration between faculty and IT staff.

Administrative Access: is defined as a level of access above that of a normal User. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. Among other things, this access includes any access that allows a user to access Personally Identifiable Information (PII).

ATS: University's Academic Technology Services Department, which reports directly to the Provost of the University.

AU Technology Resources: are assigned computer accounts, email services, and the shared University network(s), which includes resources, staff and facilities operated by the University, whether owned, leased, used under license or by agreement, including, but not limited to: telephones (including Mobile Devices) and telephone equipment, voice mail, SMS, desktop laptop computers, Mobile Devices, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computing-related contracts, network bandwidth, usernames, passwords, documentation, disks, CD-ROMs, DVDs, magnetic tapes, and other electronic media or storage devices. Email, chat, facsimiles, mail, any connection to the University's network(s) or use of any part of the University's network(s) to access other networks, connections to the Internet that are intended to fulfill information processing and communications functions, communication services, hardware, including printers, scanners, facsimile machines, any off-campus computers and associated equipment provided for the purpose of University work or associated activities.

Authorized User(s) or Users: are all users of Technology Resources including, but not limited to, employees, temporary employees, faculty, students, alumni, campus visitors, contractors, vendors, consultants and their related personnel, and other users authorized by the University to access its systems and networks.

CIO: is the University's Chief Information Officer.

Cloud Computing: encompasses utilizing any external storage, computing, software services, or hosting environment that is not directly controlled by University.

Copyright Act of 1976: The Copyright Act of 1976 is a United States copyright law and remains the primary basis of copyright law in the United States, as amended by several later enacted copyright provisions.

Covered Accounts: includes accounts that the University offers or maintains that involves or is designed to permit multiple payments or transactions; and any other account that the University offers or maintains for which there is a reasonably foreseeable risk to students or to the safety and soundness of the University from identity theft, including financial, operational, compliance, reputation or litigation risks. The University is a creditor for the purpose of FACTA because in certain circumstances the University defers payment for services. As a Creditor, the University has determined that it maintains the following Covered Accounts: The Perkins Loan Program, Institutional Loan Accounts, and Student Receivables.

Critical Data: Any user or application data directly related to business continuity and or any data being retained for regulatory compliance reasons.

Critical Device: Any University owned hardware device used to conduct data within the University Network.

Customer: any individual (student, parent, faculty, staff, or other third party with whom the University interacts) who receives a financial service from the University and who, in the course of receiving that financial service, provides the University with Personally Identifying Information about themselves.

Data Security Incident: occurs when there is a serious threat of or unauthorized access or acquisition to University Technology Resources or an Authorized User's computerized data that compromises the security, confidentiality, or integrity of the information, including institutional data. A data security incident also occurs where there has been unauthorized access or acquisition of encrypted data and the confidential process or key to the encryption is also compromised. Data Security Incidents can range from the unauthorized use of another user's account or system privileges to the execution of malicious code, viruses, worms, Trojan horses, cracking utilities, or attacks by crackers or hackers. Data Security Incidents may also involve the physical theft of University Technology Resources or an Authorized User's technology, such as a computer or other electronic media, or may occur as the result of a weakness in information systems or components (e.g., hardware design or system security procedures).

A non-exhaustive list of symptoms of incidents that qualify as Data Security Incidents include:

1. A system alarm or similar indication from an intrusion detection tool;
2. Suspicious entries in a system or network accounting;
3. Accounting discrepancies; unexplained new user accounts or file names;
4. Unexplained modification or deletion of data; system crashes or poor system performance;
5. Unusual time of usage; and
6. Unusual usage patterns.

Good faith acquisition of PII by a user granted administrative access pursuant to the University FERPA Policy does not constitute a Data Security Incident, provided that the PII is not used or subject to unauthorized disclosure.

Directory Information: means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. University designates the following categories of student information as public, or directory information: name, graduation date, degree granted, enrollment status (current students) dates of attendance, and major. The University may disclose such information for any purpose, at its discretion. Currently enrolled students may withhold disclosure of any category of information under FERPA. To withhold disclosure, written notification must be received in the Office of the Registrar. University assumes that failure on the part of any student to specifically request the withholding of categories of directory information indicates individual approval for disclosure.

DHCP: (Dynamic Host Configuration Protocol) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

Digital Millennium Copyright Act (P.L. 105-304) (DMCA): a 1998 amendment to the Copyright Act of 1976 that establishes certain limitations of copyright infringement liability for online service providers (OSPs), including colleges and universities, when certain requirements are met by the OSP. The Act contains a number of other provisions, including prohibitions on circumvention of technological protection measures among others.

DMCA Notice or Takedown Request*:* a warning or request issued from a copyright holder or a representative of the copyright holder. These copyright holders have identified computers on the University's network as having potentially violated the DMCA and issue warnings regarding the particular infringement to the University.

Employee Financial Information: that information the University has obtained from an employee in the process of offering a benefit or service. Offering a benefit or service includes all University sponsored benefit plans and University financial services such as flexible spending accounts, and personal payroll services. Examples of employee financial information include bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

Encrypted Data: refers to information that has been converted through software into a non-human readable form typically via a password or phrase (which is also used to decrypt the file when the information is to be accessed). All encryption must conform to prevailing industry standards.

ePHI: Electronic protected health information refers to any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.

FCRA: Fair Credit Reporting Act is U.S. Federal Government legislation enacted to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies.

Federal Trade Commission (FTC): is an independent agency of the United States government, established in 1914 to prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity.

FERPA: the Family Educational Rights and Privacy Act of 1974, which is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Fair and Accurate Credit Transactions Act of 2003 (FACTA): is an amendment to FCRA (Fair Credit Reporting Act) that was added, primarily, to protect consumers from identity theft.

FIPS: Federal Information Processing Standards developed by NIST (National Institutes of Standards and Technology) when compelling requirements such as for security exist and there are no acceptable industry standards or solutions. https://www.nist.gov/itl/popular-links/federal-information-processing-standards-fips.

GBL: The Gramm–Leach–Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.

Higher Education Act (HEA): HEA requires higher education institutions to report and disclose information from various administrative areas and make its information readily available to interested parties via this website

Higher Education Opportunity Act of 2008 (HEOA): The Higher Education Opportunity Act (Public Law 110-315) (HEOA) was enacted on August 14, 2008, and reauthorizes the Higher Education Act of 1965, as amended (HEA).

HIPPA: the Health Insurance Portability and Accountability Act of 1996 is United States legislation that provides data privacy and security provisions for safeguarding medical information.

Identity theft: means fraud committed or attempted using the identifying information of another person without authority.

Incident Response Team: is a group of individuals who will provide a quick, effective, and orderly response to a data security incident. The incident response team's mission is to prevent the misappropriation of confidential information such as PII, damage to the University information technology, serious loss of profits, public confidence, or information assets by providing an immediate,

effective, and skillful response to any unexpected event involving computer information systems, networks, or databases. Members of the incident response team will include the CIO, the University's general counsel, designated Information Technology staff, and may include a forensic specialist outside of the University who will provide independent analysis of any data security incident, and any additional individuals deemed appropriate by the University.

Information Technology: means IU computing resources, information technologies, and networks, including but not limited to, computers, computing staff, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computing-related contracts, network bandwidth, usernames, passwords, documentation, disks, CD-ROMs, DVDs, magnetic tapes, and other electronic media or storage devices.

Institutional Data: is any information, including Information, PII, and student and employee financial information, and Public Information that can be linked to any individual, including but not limited to, students, faculty, staff, patients, or contractors. Institutional data and all applications storing and transmitting such data, regardless of the media on which they reside, are valuable assets, which AU has an obligation to manage, secure, and protect.

Internet Service Provider (ISP): A business or organization that offers user(s) access to the Internet and related services.

ISP: Internet Service Provider.

IT: The University's Information Technology Department which reports directly to the Vice President of Finance and Treasurer of the University**.**

IT Advisory Committee: provides overall guidance and direction, reviews high impact projects, and arbitrates disparate requests for IT resources.

IT Steering Committee: works with the Vice Presidents of the University to approve strategic direction and funding for IT.

IT Network Resource: Any resource made available and managed by IT over the University network.

Lasting Value: email message information that should be retained due to operational nature of the message content. Lasting value also describes email messages under retention schedules for which the retention time period has lapsed.

Log-in Credentials: University assigned username and private personal password.

Mobile Device: any handheld or portable computing device including running an operating system optimized or designed for mobile computing. Any device running a full desktop version operating system is not included in this definition.

Nonpublic Customer Information: any information (i) a student or other third party provides in order to obtain a financial service from the University, (ii) about a student or other third party resulting from any transaction with AU involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person. Nonpublic Customer Information may be in paper, electronic, or other form.

Official University Webpages*:* Official University webpages are those that have been created by the University, its colleges, schools, departments or other administrative unit, for official University business.

Official University Websites*:* Websites that are sponsored by University.

Patch: A piece of software designed to fix problems with or update a computer program or its supporting data.

Peer-to-Peer: a network environment where participants share their resources (such as files, disk storage, or processing power) directly with their peers without having to go through an intermediary network host or server.

Peer-to-Peer File Sharing Applications and Programs: programs or services that use peer-to-peer technology to share music, movies, software, or other digitally stored files.

Personally Identifiable Information (PII): PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity that has not been designated as directory information, such as social security number, place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Private Network Resource: A resource or service provided to on-campus clients but is not available to individuals accessing the University's network from the Internet.

Public Information: is information, including directory information (unless a student has expressly requested non-disclosure pursuant to the University FERPA Policy) that is available to the general public.

Red Flag: is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Remote Access: The ability to Log-in to a network from a distant location.

Remote Access Connection: A secured private network connection built on top of a public network, such as the Internet.

Remote Wipe: the ability to erase all data on a device when the user and the device are physically separated. This is most often done through a service that the manufacturer provides via a website.

Resource: Any hardware or software purchased for academic or administrative use at the University.

Retained Records: email messages that contain content subject to the University's Schedule. Examples can be found in the University Records Retention Section.

Security Patch: a fix to a program or application that eliminates a vulnerability exploited by malicious hackers. Most Mobile Devices will notify the user of updates to their installed applications that include the latest vulnerability fixes.

Social Media: includes the various online technology tools that enable people to communicate easily via the Internet to share information and resources. Social media can include blogs and social networking sites like Facebook, Twitter, Instagram, YouTube, and LinkedIn. Any Web application, site, or account maintained by University that facilitates an environment for employees, students, and alumni to share information and opinions in an interactive way is included in this definition.

Student Financial Information: that information the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of student financial information include bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

Technology Resources: Technology Resources are assigned computer accounts, email services, and the shared University Network which includes resources and facilities operated by the University, whether owned, leased, used under license or by agreement, including, but not limited to: telephones (including Mobile Devices) and telephone equipment, voice mail, SMS, mobile data devices, desktop and laptop computers. Email, chat, facsimiles, mail, any connection to the University's network or use of any part of the University's network to access other networks, connections to the Internet that are intended to fulfill information processing and communications functions, communication services, hardware, including printers, scanners, facsimile machines, any off-campus computers and associated equipment provided for the purpose of University work or associated activities.

Transitory: routine communication, scheduling, or any messages not deemed to have Lasting Value. Examples include meeting or event notices, internal requests for information, announcements, or unsolicited commercial email (spam), etc.

Trojan: A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions.

University: is Arcadia University its colleges, schools, affiliates, division, and subsidiaries.

User Managed Service: A service where the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

User Support Team: Is the University helpdesk (helpdesk@arcadia.edu).

Virtual Private Network (VPN): A secure connection to a private network through a public network.

Virus: A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

Wireless Access Point: Is a hardware device which sends and receives wireless traffic to and from nearby wireless clients.

Worm: A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

xxxx: is the University's single sign-on password needed to access campus computers, Wi-Fi, My AU, Canvas, Power Campus, and many other enterprise systems.

V. ENFORCEMENT

The University considers violations under this Policy to be serious offenses and will take such action it deems necessary to protect its network from events that threaten or degrade operations. The University reserves the right to disconnect or disable, without warning or prior notice, any computer,

account, or service that poses a security or performance threat to University resources or services or that otherwise violates University policies. Access may be later restored after the incident has been reviewed and the risk mitigated or eliminated. Any Authorized User found to have violated this Policy may be subject to disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University or investigation and/or prosecution by the appropriate local, state, or federal authorities. All users will assume full liability, legal, financial or otherwise, for their actions.

VI. EFFECTIVE DATE

This interim Policy is effective on the date signed by the President.

VII. SIGNATURE, TITLE AND DATE OF APPROVAL

By: N. deVille Christmas
President

Date: 3/29/17